THESIS / THÈSE

MASTER EN SCIENCES INFORMATIQUES

Elaboration d'une méthodologie orientée-principes pour la modélisation business de la vie privée sur base de textes légaux

Kupper, Thomas

Award date:
2017

Awarding institution:
Universite de Namur

Université de Namur
Faculté d'informatique
Année académique 2016–2017

Élaboration d'une méthodologie orientée-principes pour la modélisation business de la vie privée sur base de textes légaux

Thomas Kupper

Maître de stage : Chrisophe Feltus

Promoteur : Jean-Noël Colin

Mémoire présenté en vue de l'obtention du grade de
Master en Sciences Informatiques.

Résumé

Résumé

Avec l'augmentation constante du volume d'informations à caractère privé collectées et traitées, il devient de plus en plus important de protéger les individus. Le *règlement général sur la protection des données* (GDPR), mis en place par l'Union Européenne, imposera dès 2018 de nouvelles règles à tout acteur traitant et collectant des données à caractère personnel. Ce mémoire présente une méthodologie de création de modèles au niveau business (organisationnel) en conformité avec un texte légal. Une application de cette méthodologie appliquée au GDPR est présentée, afin de fournir un outil à ces acteurs.

Mots-clés : modèle orienté-principes, gestion de la vie privée, GDPR, méthodologie de modélisation, conformité légale, modèle.

Abstract

With constantly increasing volume of collected and processed private data, it becomes more and more important to protect individuals. The *General Data Protection Regulation* (GDPR), implemented by European Union, will enforce as of 2018 new regulations to any actor processing or collecting personal data. This Master Thesis presents a methodology to create models at a business level (organizational) in compliance with a legal text. An application of this methodology to the GDPR is presented, in order to provide a tool to those actors.

Keywords : principles-oriented model, privacy management, GDPR, modeling methodology, legal compliance, model.

Remerciements

Je voudrais tout d'abord remercier mon promoteur le professeur Jean-Noël Colin pour sa compréhension pendant mon stage, qui a été mouvementé, et pour son soutien. Mais également pour m'avoir permis de réaliser d'avoir de belles opportunités pendant ce stage, notamment d'assister à la conférence Modelsward 2017. Et également pour sa relecture et ses conseils durant la rédaction de ce mémoire.

Je voudrais aussi remercier Christophe Feltus pour son accompagnement durant mon stage, sa confiance en moi, son dynamisme et le temps qu'il a consacré à revoir mon mémoire et mes recherches. Je voudrais aussi lui exprimer ma reconnaissance pour m'avoir offert l'opportunité de défendre son travail à la conférence Modelsward 2017.

Merci à Florian, Anne, Pierre, Antoine et ses lamas, Jonathan et Jérémy d'avoir été mes compagnons de galère à la faculté d'informatique.

Je remercie également mes parents pour leur soutien durant la rédaction de ce mémoire, et pendant toutes mes études en général.

Merci à Joanne pour ses encouragements et sa merveilleuse présence.

Enfin, je dédie ce mémoire à ma soeur Elise.

Table des matières

Table des figures

Glossaire

Autorité de contrôle = "une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51" du GDPR [2].
Controller = voir "responsable du traitement".
Considérant = "Chacun des alinéas d'un arrêt d'une cour et des décisions des juridictions administratives, qui commence par les mots considérant que et qui motive la décision." [1]
Data subject = voir "personne concernée".
FCL = Formal Contract Language.
GDPR = General Data Protection Regulation *ou* Règlement général sur la protection des données.
LIST = Luxembourg Institute of Science and Technology.
Personne concernée = personne identifiée ou identifiable grâce à une ou plusieurs donnée(s) la concernant. "Data subject" en anglais.
Privacy = voir "vie privée".
Processor = voir "sous-traitant".
Sous-traitant = "la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement" [2].
Responsable du traitement = "personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement" [2]. "Controller" en anglais.
Vie privée = "capacité, pour une personne ou pour un groupe de personnes, de s'isoler afin de protéger ses intérêts". [2]

1. `http://www.larousse.fr/dictionnaires/francais/consid\%C3\%A9rant/18384` ; Consulté le 18/05/2017
2. `https://fr.wikipedia.org/wiki/Vie_priv\%C3\%A9e` ; Consulté le 18/05/2017

Chapitre 1

Introduction

Dans un monde de plus en plus connecté, où le volume de données personnelles récoltées et traitées augmente sans cesse, la question de la vie privée devient un enjeu majeur. L'Union Européenne met donc en place un règlement afin de réguler le traitement et la collecte de données. Les entreprises vont devoir très vite s'y conformer puis qu'il entre en vigueur dès mai 2018. Elles ont donc besoin d'outils, notamment de modèles de gestion de ce nouveau règlement, afin de mettre en place ces exigences. Ce présent mémoire tente d'apporter une solution originale en créant une méthodologie de modélisation conforme aux textes légaux, et l'applique à ce règlement.

L'objectif de ce chapitre est de présenter le contexte dans lequel s'inscrit ce mémoire ; suivi d'une explication de la problématique, de l'objectif du stage et d'une explication brève sur l'outil utilisé dans le cadre de ce travail. Enfin, une conclusion sur les objectifs sera présentée.

1 Contexte

Ce mémoire est la suite d'un stage effectué au sein du centre de recherche du *Luxembourg Institute of Science and Technology* (LIST), à Belval au Luxembourg. Il s'inscrit dans le cadre d'un projet mené sur les questions de la vie privée.

1.1 Pourquoi étudier la vie privée ?

Pour quelle raison étudier la vie privée dans le cadre de l'ingénierie logicielle ? Le monde numérique dans lequel nous vivons soulève de plus en plus de questionnements et d'inquiétudes quant à l'utilisation de données à caractère privé. Leur volume augmente sans cesse à cause de : la multiplication

des appareils connectés (IoT, smartphones, tablettes...), de la quantité de données collectées et traitées (big data, deep learning...), du ciblage marketing, etc. L'utilisation de toutes ces données n'est pas toujours claire pour l'utilisateur, et, la plupart du temps, il ignore ce qui est fait de ses données personnelles.

La question de la vie privée devient donc un enjeu important dans l'informatique d'aujourd'hui.

1.2 Cadre légal

Un cadre légal en harmonie avec ces nouveaux enjeux numériques est maintenant nécessaire. C'est ce que l'Union Européenne a mis en place en introduisant le Règlement général sur la protection des données, ou *General Data Protection Regulation* (GDPR) en anglais, qui entrera en vigueur en mai 2018. L'objectif de ce règlement est d'uniformiser les règles, d'améliorer la sécurité juridique et de renforcer la confiance dans le marché du numérique [15]. Il abroge la Directive 95/46/EC qui s'appliquait à la protection des données jusqu'alors.

NB : une directive est une note de l'Union Européenne que les états membres doivent respecter et en fonction de laquelle ils doivent adapter leurs lois pour la respecter. Un règlement, à l'inverse, est applicable directement pour les états membres.

2 Problématique

Ce règlement (GDPR) est l'un des règlements les plus importants de ces dernières années [7], et son approche n'est donc pas aisée pour les entreprises qui devront bientôt s'y conformer, sous peine d'amendes importantes [1]. Souvent, cela leur impose une restructuration de leurs systèmes, ou tout du moins des modifications majeures, si l'entreprise n'est pas encore conforme à ces nouvelles exigences légales. Cependant, mettre en place ces exigences présente des défis importants à cause du caractère transversal et étendu de la régulation sur le traitement des données. Cette dernière s'applique à de nombreux niveaux et sur de nombreuses structures, ce qui peut rendre son implémentation compliquée pour les acteurs des entreprises.

1. Article 83 du GDPR

3 Stage

Le travail qui a été effectué lors du stage trouve son origine dans un article rédigé par Feltus et al. [16] qui ont créé un méta-modèle pour le management de la vie privée au sein d'une entreprise, sur base du travail d'Alter. Ce dernier mettait en évidence trois grands concepts : les ressources, les rôles et les activités. L'approche de Feltus et al. a été la suivante : il faut considérer la vie privée comme un élément de management inclus dans l'ensemble des activités de l'entreprise. Ils présentent donc le méta-modèle à la figure 3.4 qui montre bien que les activités liées à la vie privée sont des activités faisant partie intégrante de l'entreprise.

Le méta-modèle met en exergue la place de la gestion de la vie privée au sein des activités de l'entreprise. Le travail durant le stage consistait à modéliser plus concrètement cette gestion de la vie privée, sur base des textes légaux, et en premier lieu sur base du GDPR.

L'objectif de cette modélisation en conformité avec le GDPR est de servir d'outil d'évaluation de conformité d'une entreprise avec le modèle, et donc avec le cadre légal.

4 ArchiMate et modélisation en couches

La modélisation dans ce mémoire est faite sur base d'un outil nommé Archimate (version 3.0), qui est un langage de modélisation pour décrire des architectures d'entreprises. Ce langage est basé sur un système en couches. Une couche est définie comme : « une abstraction du framework d'Archimate à laquelle une entreprise peut être modélisée » [1].

Archimate définit trois couches principales : business, application et technologie ; avec trois aspects possibles : passif, comportement et actif (voir Figure 1.1). Il définit également un framework enrichi qui ne sera pas discuté ici mais dont l'un des éléments est important pour cette analyse : la motivation.

Voici une description succincte des couches citées :

— La couche motivation représente les motivations ou les raisons qui guident le design d'une entreprise.

— La couche business sert à modéliser l'architecture business d'une entreprise. L'architecture business est définie comme : "un modèle de l'entreprise qui fournit une compréhension commune de l'organisation et est utilisé pour aligner les objectifs stratégiques et les exigences tactiques."[48]

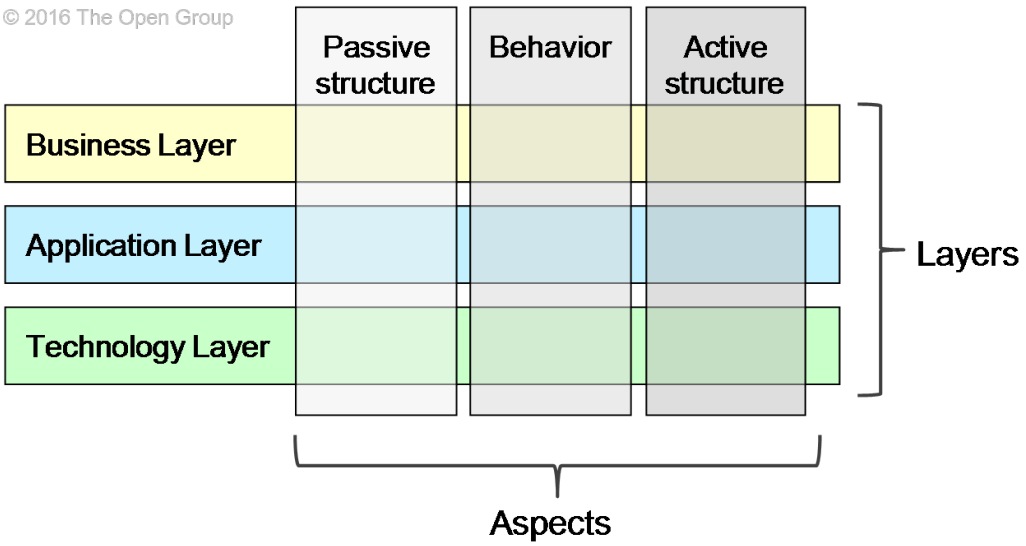

FIGURE 1.1 – Modèle en couches défini par ArchiMate 3.0

— La couche application permet de modéliser l'architecture des systèmes d'information d'une entreprise.
— La couche technologie permet de modéliser l'architecture technologique d'une entreprise.

Toutes ces couches peuvent avoir des interactions entre elles afin de représenter au mieux une vue de l'entreprise. Un exemple [2] de modèles en plusieurs couches se trouve à la figure 1.2. Le travail de ce mémoire se repose en grande partie sur cette structure en couches.

5 Orienté-principe

L'originalité de l'approche de la méthodologie présentée dans ce mémoire est sa modélisation **orientée-principe** des textes légaux. Le but est de déterminer les grands principes qui régissent le domaine d'étude, la vie privée dans ce cas, et d'extraire les éléments légaux qui concernent ce principe. Cela est discuté plus en détail dans le chapitre 3.

6 Objectifs

En conclusion, les objectifs sont :

2. `http://www.archimate.nl/en/about_archimate/example.html`

1. Sur base de la méthodologie développée durant le stage, élaborer une méthodologie pour modéliser la vie privée au niveau de la couche business, sur base de textes légaux.
2. Appliquer cette méthodologie au cas du GDPR.

7 Structure de ce mémoire

Ce mémoire va être structuré comme suit. Tout d'abord un état de l'art est présenté au chapitre 2. Ensuite, la méthodologie développée dans ce mémoire est expliquée au chapitre 3. Le chapitre 4 présente d'une part l'extraction et l'articulation des concepts légaux (section 1 et 2) et d'autre part l'instance appliqué au GDPR (sections 3 et suivantes). Enfin, ce mémoire se termine avec une discussion, une conclusion et une présentation de possibles travaux futurs au chapitre 5.

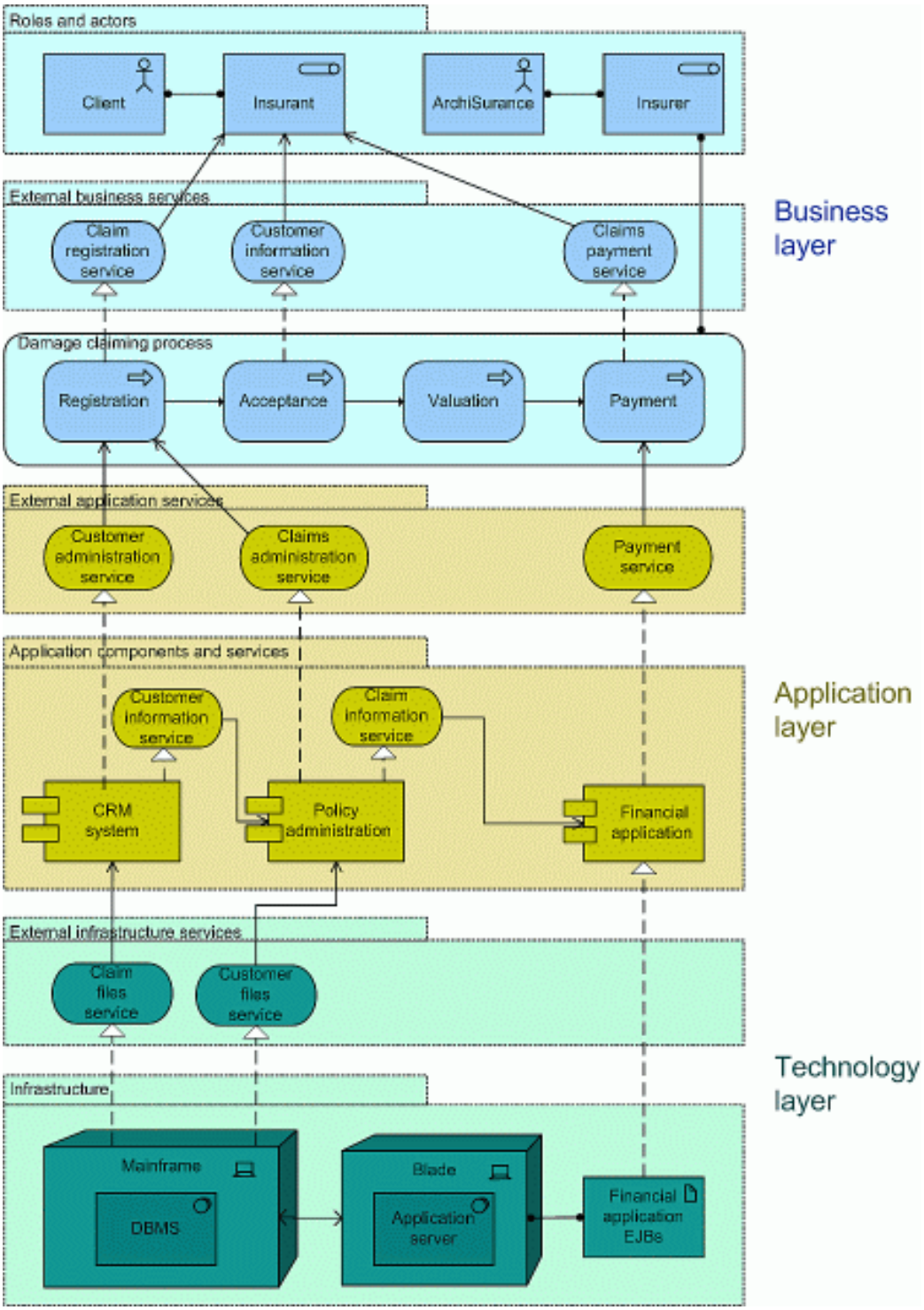

FIGURE 1.2 – Exemple de modèle en couches modélisé à l'aide d'ArchiMate

Chapitre 2

Etat de l'art

Le sujet de ce mémoire se trouve à l'intersection de trois domaines différents. Ces domaines sont la **vie privée**, la **modélisation business** et la **modélisation de textes légaux**. Chacun de ces domaines va donc être discuté dans cet avant-propos

Il faut tout d'abord noter que la vie privée n'est pas inévitable dans ce travail. En effet, la méthodologie élaborée ici ne se destine pas uniquement à la modélisation de la vie privée, mais aussi à d'autres domaines. Néanmoins, il semble tout de même important de présenter, dans ce cadre, quelques articles afin d'introduire le sujet.

D'autre part, il est clair que la limite entre les domaines de la modélisation business et la modélisation de textes légaux est assez ténue. Mais il faut noter que dans "Modélisation des textes légaux", est entendu l'extraction et l'atomisation des règles légales, qui se distingue de la modélisation business.

Enfin, d'autres enjeux apparaissent également : notamment pour la vie privée qui posent beaucoup de questions éthiques ou légales. De la même manière, les aspects légaux peuvent trouver certaines sources dans le domaine du droit.

Il est à noter qu'une partie de cette recherche dans la littérature scientifique se trouve à l'intérieur même de la méthodologie, qui se base sur les principes trouvés dans cette dite littérature. C'est le cas, par exemple, du consentement dans ce mémoire (section 4.6 du chapitre 4).

1 Vie privée

La question de la vie privée peut se poser à plusieurs niveaux. Pour reprendre le concept de modèle en couches présentées dans la section 4 du chapitre 1, la question de la vie privée peut s'appliquer à ces différents ni-

veaux. Dans la suite, une première partie discutera de la vie privée au niveau de la couche applicative (de bas niveau), et une seconde discutera de la vie privée au niveau de la couche business ou même au niveau motivation (de haut niveau).

Les articles dans la section qui suit ont été sélectionnés sur base de la reconnaissance des pairs (nombre de citations notamment). Néanmoins, pour la section 1.2, les articles ont été sélectionnés sur base de leur pertinence par rapport au sujet, en particulier dans ce domaine où la vie privée au niveau business est encore assez peu étudiée.

1.1 La vie privée au bas niveau

Domingo-Ferrer, notamment, présente dans [11] les 3 dimensions de la vie privée au niveau des bases de données :

- *Respondent privacy* : consiste à éviter de ré-identifier les personnes à un enregistrement dans une base de données ;
- *Owner privacy* : qui concerne deux ou plusieurs entités qui peuvent communiquer via des requêtes sur leurs bases de données de manière à ce que seuls les résultats des requêtes sont révélés ;
- *User privacy* : qui concerne la garantie de la vie privée des requêtes effectuées par une personne, afin d'éviter le profilage ou la ré-identification.

Il désigne également les protections pour chacun de ces enjeux par respectivement :

- *Statistical Disclosure Control* mené par les statisticiens ;
- *Privacy-Preserving Data Mining* mené par la communauté cryptographique ; et,
- *Private Information Retrieval* également mis en place par la communauté cryptographique.

Il termine en montrant que ces trois protections sont indépendantes les unes des autres.

Dans le même ordre d'idée, mais de manière plus large, De Capitani Di Vimercati et al. présentent dans leur article *Data privacy Definitions and techniques* [10] un panorama des principales techniques proposées dans la littérature pour protéger la vie privée des utilisateurs dans la publications des données.

Ils distinguent deux grandes catégories : les techniques plus traditionnelles qui adoptent une définition syntaxique de la vie privée et les propositions plus récentes qui ont, elles, une approche sémantique. Les premières reposent principalement sur des évaluations numériques, pouvant causer la ré-identification des personnes par exemple. Les secondes reposent sur les mécanismes de publication en eux-mêmes qui peuvent impacter les personnes

présentes dans un ensemble de données, mais aussi ceux qui n'y sont pas, via d'autres déductions.

Ils présentent également les quatre types d'attributs qui peuvent être présents lors de la publication d'une table de *microdata* [41] : identifiants, quasi-identifiants, attributs confidentiels et attributs non-confidentiels.

Les techniques syntaxiques peuvent également avoir deux scénarios différents : non-interactif, il y a publication d'un ensemble de données et la vie privée est protégée à la génération ; interactif, un ensemble de requêtes est effectué sur un ensemble de données, la protection réside alors dans l'ensemble des réponses des requêtes.

Enfin, ils présentent les techniques de *k-anonymity*, de *l-diversity* et de *t-closeness*.

La *k-anonymity* [41] est une propriété applicable à un ensemble de données. Un ensemble de données est dit k-anonyme si l'information pour chacun des individus contenus dans la publication des données ne peut pas être distingué d'au moins k-1 individus dont les informations apparaissent aussi dans la publication.

La *l-diversity* [31] repose sur les vulnérabilités de la k-anonymity. Une personne ayant une connaissance antérieure sur un sujet peut le retrouver dans un ensemble de données malgré la k-anonymity. La l-diversity est donc un framework qui vient renforcer la k-anonymity en réduisant la granularité d'une publication de données.

La *t-closeness* [29] vient également renforcer la k-anonymity. Cette dernière ne protège pas suffisamment contre la divulgation d'attributs. La t-closeness s'assure que chaque publication a au moins t valeurs bien représentées pour chaque attribut sensible.

D'autre part, la vie privée s'applique à d'autres domaines de la sécurité comme le contrôle d'accès. Présenté dans l'article [4], Ardagna et al. met en place un système de *Privacy-aware policies* pour le contrôle d'accès, la publication et le traitement des données. D'autres appliquent ces intérêts de vie privée sur la localisation, comme [39] ou [12] par exemple. Ou encore, sur les questions de vie privée dans le cloud, comme Wang et al. [49] le présentent dans un système d'*auditing* public préservant la vie privée.

En conclusion, la vie privée est présente dans plusieurs domaines de la sécurité et divers auteurs tentent de trouver des solutions au niveau applicatif ou opérationnel pour répondre à cette problématique.

1.2 La vie privée au plus haut niveau

Au-delà de la problématique applicative, la vie privée soulève des questions d'ordre business ou de gestion, voire légal ou éthique. Ces deux derniers

points étant hors du cadre de ce travail, ils ne seront pas discutés.

La littérature à ce sujet est moins fournie que celle sur la question précédente.

Le projet EnCoRe [33] propose un *framework* avec une solution très intégrée (solution technique reprenant de nombreux éléments de la vie privée cité dans la section 1.1), et adopte donc une vision assez large de la problématique, sans pour autant interroger les fondements de gestion de sa solution.

Cavoukian et al. dans [9] présentent sept principes fondateurs de la *Privacy by design*, c'est-à-dire : réfléchir à la vie privée dès la conception. Ces principes sont les suivants :

1. Proactive pas réactive et préventive pas réactive : c'est-à-dire qu'on observe l'adage qui dit "mieux vaut prévenir que guérir" ;
2. La vie privée comme responsabilité par défaut ;
3. La vie privée intégrée au design ;
4. Toutes les fonctionnalités : une organisation qui met en place la vie privée, crée de la valeur tout en protégeant les utilisateurs ;
5. Protection de bout en bout du cycle de vie ;
6. Visibilité et transparence : l'organisation doit être ouverte et honnête vis-à-vis des utilisateurs ;
7. Respect de la vie privée de l'utilisateur : tous les processus doivent être cohérents avec la vie privée.

Antón et al. présentent dans [3] une gestion complète de la vie privée en ligne. Ils séparent cette gestion en 4 parties distinctes, comme indiqué à la figure 2.1 : le côté entreprise, le côté utilisateur, l'aspect utilisabilité et les influences sociétales, légales ou économiques. Le côté entreprise est séparé en 2 branches : l'une concerne les outils et les algorithmes tandis que l'autre met en place des modèles. Cette seconde branche est séparée en couches, qui représentent un premier aperçu sur la structure proposée dans la méthodologie présentée dans ce mémoire (voir chapitre 3).

2 Modélisation Business

L'un des objectifs de ce mémoire est de créer une méthodologie menant à une modélisation de la vie privée. Il est donc nécessaire d'évaluer les méthodes permettant de modéliser des éléments au niveau business ou au niveau motivation.

Les articles de cette section ont été choisis sur base de leur pertinence ainsi que leur reconnaissance dans le monde scientifique.

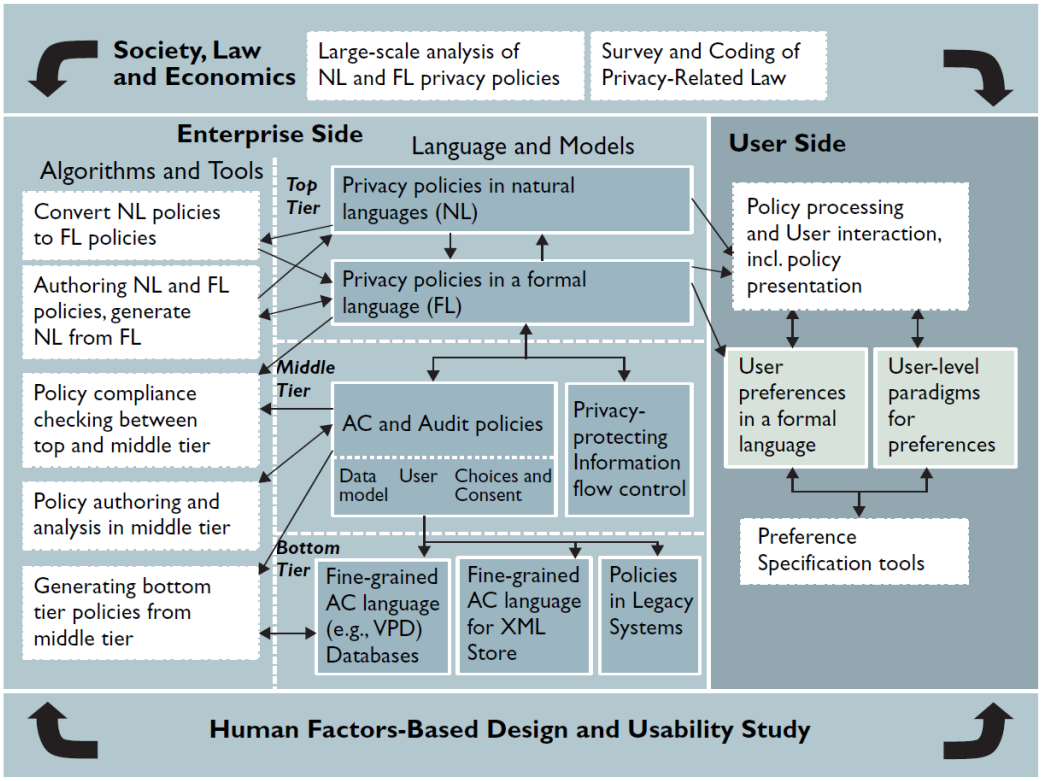

FIGURE 2.1 – Schéma de l'architecture de Anton et al. [3]

L'un des problèmes en IT est la rencontre des exigences de haut-niveau [47]. Le framework i* tente de répondre à cette question grâce à un modélisation en arbre de *goals* [52], en se concentrant sur la motivation ou le "pourquoi" de l'utilisateur. D'un point de vue différent, Gordijn et al. présente dans [22] le modèle e3-value qui tente de réconcilier les processus business avec l'IT, en évitant l'aspect technique intégré dans la solution haut niveau. Ces points de vue peuvent se rencontrer, comme cela est démontré dans [23] où l'intégration de i* (ce que veulent les acteurs) et de e3-value (les échanges économiquement viables pour l'entreprise) établit un processus combinant les deux modèles.

D'autres auteurs tentent d'adapter des modèles pour combler ce besoin de modéliser le niveau business, comme Eriksson et Penker qui ont adapté UML pour intégrer des notions business et donc mieux répondre aux exigences IT [14].

Encore d'autres auteurs fusionnent divers modèles afin de remplir ce besoin de relier l'IT et le business. Fitscher et Pigneur ont créé un modèle

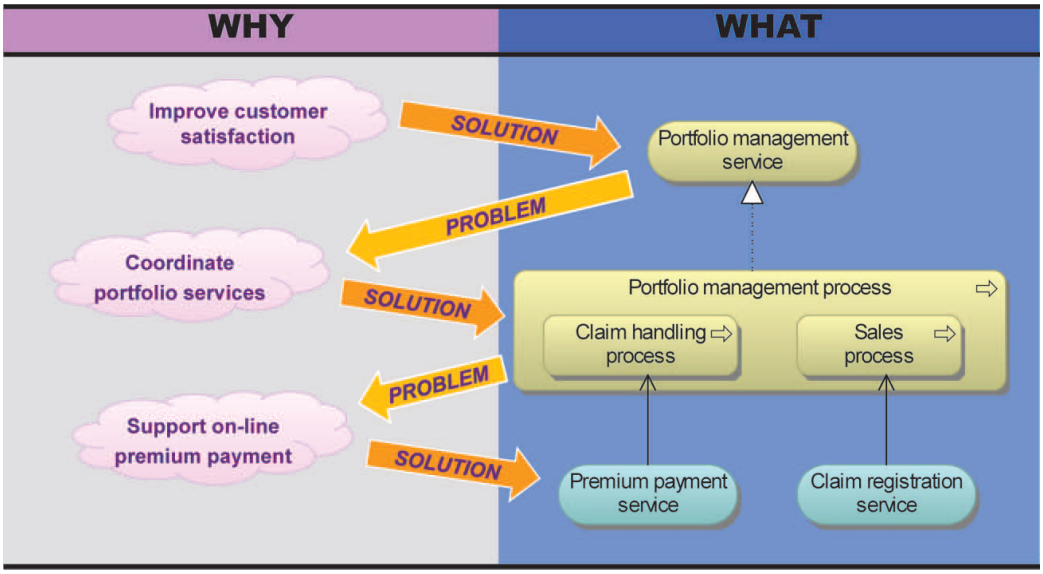

FIGURE 2.2 – Modèle en couches d'Engelsman et al. [13]

commun au *Business Model Canevas*[37] et à l'architecture d'une entreprise (modélisé avec ArchiMate) [17]. Engelsman et al. [13] ont, quant à eux, présenté un langage de modélisation –nommé ARMOR– pour étendre l'architecture d'entreprise avec des exigences et des goals business. Ce langage est construit en couches d'abstraction avec deux vues : l'une sur la motivation (*why*) et l'autre sur la partie orientée solution (*what*), comme cela est illustré à la figure 2.2.

Enfin, dans le même ordre d'idées, Ullah et Lai présentent des exigences en utilisant un arbre de *goals* [47] sur plusieurs couches : décision, management, opérationnel et IT opérationnel (voir figure 2.3).

3 Modélisation des textes légaux

Les méthodes de modélisation de textes légaux sont structurées généralement en plusieurs étapes : l'extraction des concepts légaux, leur atomisation et la modélisation, avec possiblement un traitement supplémentaire lors de la modélisation (pour l'adapter à un langage particulier par exemple).

L'atomisation est une étape qui consiste à extraire les règles légales d'un texte de loi et à les réduire à une déclaration simple, dite "atomique", où une seule information est donnée. Il est ensuite plus simple de manipuler ces déclarations réduites pour créer des modèles.

Dans la suite, une comparaison de divers frameworks va être présentée sui-

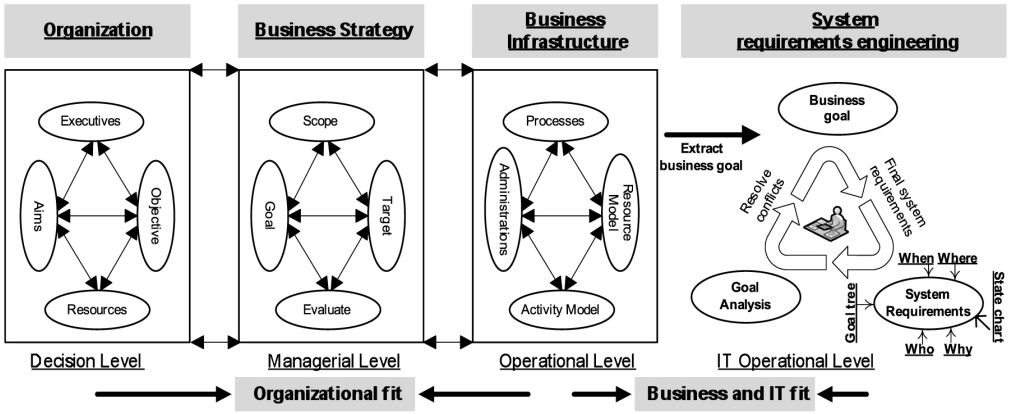

FIGURE 2.3 – Modèle en couches de Ullah et Lai [47]

vant ces critères : types d'atomisation ou de formalisation des textes légaux, contexte et particularités.

3.1 Atomisation ou formalisation des textes légaux

Cette sous-section présente les stratégies d'atomisation ou de formalisation des textes légaux mises en place par différents auteurs.

Plusieurs auteurs présentent des frameworks qui se basent sur la taxonomie de Hohfeld [25]. Cette dernière considère que toute clause légale peut être réduite à 8 concepts différents : *claim, duty, privilege, no-claim, power, liability, immunity et disability*, qui ont été réduites par Nomos en 4 concepts : *PrivilegeNoclaim, ClaimDuty, PowerLiability et ImmunityDisability* [42] [21] [43].

Lu et al. utilisent le FCL (Formal Contract Language) qui permet de représenter formellement les assertions légales [30]. Le FCL est un ensemble de propositions atomiques avec des opérations possibles : négation, obligation, permission et violation/réparation. Une proposition correspond à une déclaration.

Breaux et al. présentent un framework qui utilise le Semantic Parametrization Process, qui permet de représenter les clauses légales en prédicats logiques, puis d'en dériver les droits et les obligations [8].

3.2 Contexte

Pour la majorité des auteurs, le framwork développé peut s'appliquer à la plupart des entreprises cherchant à être en conformité avec une législation ou

des normes externes. Néanmoins, les articles [21], [43] et [8] sont plus ancrés dans un contexte de soins de santé.

3.3 Particularités

Parmi les travaux étudiés, tous présentent un objectif de conformité entre une stratégie[43] et/ou des exigences[42] d'entreprise et des contraintes légales. Néanmoins, les apports sont évidemment différents.

[30] donne une mesure de conformité entre un processus business et des contraintes légales.

[26] propose de découvrir les exigences grâce à des scénarios afin de détecter les scénarios non conformes très tôt dans le développement.

Ghanavati et al. proposent, dans plusieurs articles [19] [21] [20], une construction itérative d'un modèle basé sur un modèle de goal (GRL) et un modèle de business process (UCM). Les travaux de Ghanavati se rapprochent d'ailleurs fort de ce mémoire, et une comparaison sera discutée à la section 6.2 du chapitre 3.

3.4 Tableau de synthèse

Les sous-sections développées précédemment sont synthétisées dans le tableau 2.1, avec quelques précisions supplémentaires dans la dernières colonnes.

Articles	Atomisation	Contexte	Particularités
Siena et al.[42]	Hohfeld	Général	Un framework reprenant exigences et régulation
Ghanavati et al.[21]	Hohfeld	Santé	URN modélisé sur base de GRL et UCM
Lu et al.[30]	FCL	Général	Donne une mesure de conformité
Imeri et al.[26]	/	Général	Utilisation de scénarios
Siena et al.[43]	Hohfeld	Santé	Un framework rassemblant la stratégie de l'entreprise et les contraintes légales
Breaux et al.[8]	Semantic Parameterization	Santé	Gestion des exceptions, identification des ambiguïtés

TABLE 2.1 – Tableau de synthèse des articles de modélisation des textes légaux

Chapitre 3

Elaboration de la méthodologie

La méthodologie présentée ici utilise une méthode itérative de déploiement de modèles. C'est-à-dire qu'un premier méta-modèle est construit de manière arbitraire. Ensuite, grâce à une idée de la solution, un second méta-modèle est créé, qui est un raffinement du premier. Ce sont ces modèles qui sont raffinés au fil d'itérations jusqu'à obtenir un modèle ayant la précision et le niveau d'abstraction escompté.

1 Description du chapitre

La figure 3.1 présente visuellement la structure de ce chapitre.

Tout d'abord sera présenté un premier méta-modèle qui initie cette méthodologie à la section 2.1. Il est suivi du raffinement de ce méta-modèle à la section 2.3 sur base d'une idée non raffinée explicitée à la section 2.2.

Ensuite, la section 3 présente l'extraction des concepts légaux. Et enfin, à la section 4 présente la modélisation par principe.

Les sections 5 et 6 exposent respectivement les concepts transversaux de la méthodologie et la discussion par rapport à la double validation.

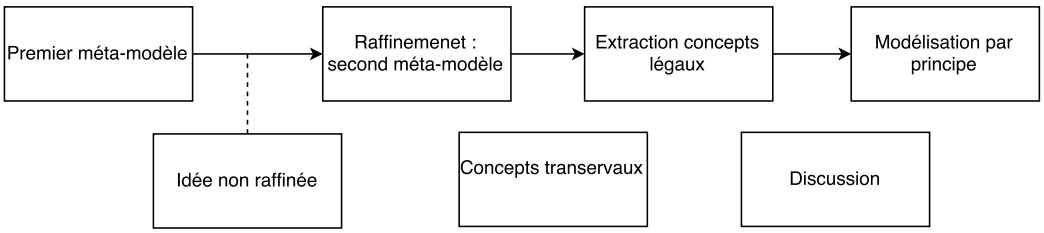

FIGURE 3.1 – Description du chapitre sur la méthodologie

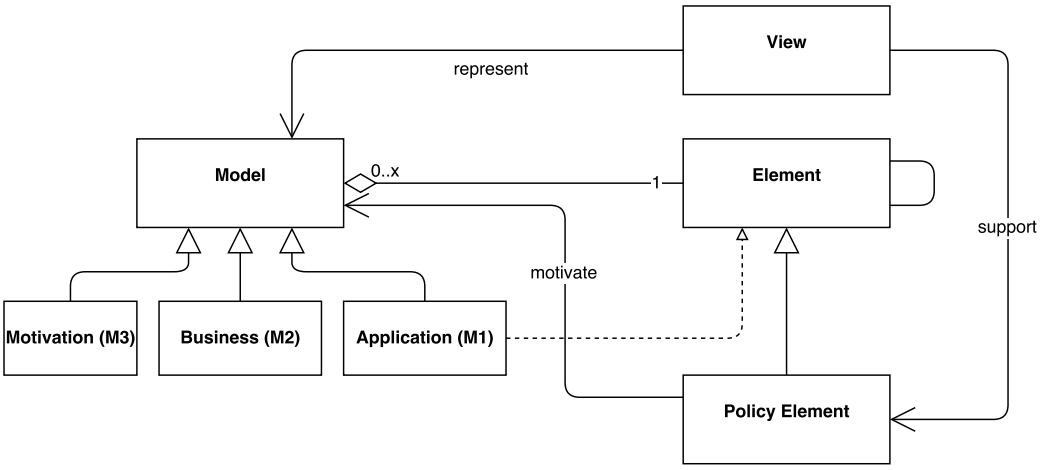

FIGURE 3.2 – Premier méta-modèle

2 Méta-modèle à plusieurs niveaux d'abstraction

2.1 Premier méta-modèle

Le premier méta-modèle (Figure 3.2) a été défini arbitrairement sur l'inspiration de ce que les textes légaux donnent comme exigences de très haut niveau.

Ce méta-modèle se base sur un ensemble de modèles en couches : motivation, business et application. Ces couches sont celles de ArchiMate 3.0 [1] adaptée à cette méthodologie. Cela est également inspiré d'auteurs présentés dans l'état de l'art (chapitre 2), notamment Ullah et Lai [47] qui ont défini une couche qui s'apparente à la motivation et qu'ils nomment *decision*.

Chaque modèle est composé de différents éléments qui ont diverses relations entre eux. Parmi ceux-ci, on trouve des éléments d'exigence (parfois nommé police dans la suite de ce mémoire). Ces derniers motivent de nouveaux modèles de couches inférieures. Enfin, on peut créer diverses vues qui représentent des modèles et supportent les éléments de police.

Par exemple, supposons un modèle de motivation : la stratégie d'une entreprise pour augmenter ses ventes. Ce modèle va motiver un modèle de niveau business pour mettre en place les processus, les objets, les acteurs... etc, qui vont modéliser cette stratégie de manière plus concrète au sein de la gestion de l'entreprise. Ces éléments vont ensuite, à leur tour, devoir être mis en place au niveau applicatif. Cette même idée est développée par Engelsman

et al. [13], comme cela a été discuté dans l'état de l'art (voir figure 2.2).

2.2 Idée non raffinée

Cette sous-section amorce la construction du méta-modèle à partir du développement d'une idée non raffinée de départ. En effet, la solution présentée ici est élaborée sur base de l'illustration d'une esquisse imprécise de la solution.

A la figure 3.3, c'est ce modèle qui est instancié. Il est composé de trois couches et de deux aspects. D'un côté, à droite, l'aspect **production** représente tout ce que fait une entreprise au niveau de son *core business*, ce qui constitue son activité principale. De l'autre côté, se trouve l'aspect **support** qui représente toutes les activités de l'entreprise qui ne concernent pas son activité principale. C'est donc, par définition, le support des activités principales. Cet aspect peut concerner, par exemple, le secrétariat, la gestion des ressources humaines... etc. Dans le cas en l'espèce, ce sont les activités liées à la vie privée et la conformité à la législation, et plus particulièrement le GDPR. De plus, cette vue peut s'inscrire en parallèle de celle de Feltus et al. [16] qui considèrent la vie privée comme faisant partie intégrante des activités de l'entreprise, et non pas comme un silo distinct des autres considérations, comme cela peut se voir sur la figure 3.4.

Les trois couches, quant à elles, sont la **motivation**, le **business** et l'**application**.

Chaque couche représente un niveau d'abstraction différent. La couche motivation concerne la considération de plus haut niveau, c'est-à-dire les exigences qui ne s'expriment pas d'un point de vue technique mais d'un objectif plus global. Cela modélise l'intention ou l'objectif d'une entreprise. Dans cette méthodologie, elle représente les exigences haut-niveau du GDPR. ArchiMate, dans ses spécifications pour la version 3.0, définit la motivation comme "les éléments utilisés pour modéliser les motivations, ou les raisons, qui guident le design ou le changement de l'architecture d'une entreprise. Il est essentiel de connaître les facteurs, souvent référé comme des *drivers*, qui influencent d'autres éléments de motivation." [1]

Les exigences du niveau motivation motivent des exigences de niveau inférieur : le niveau Business. Il concerne l'ensemble des éléments qui permettent de modéliser l'architecture d'une entreprise, comme les processus, les acteurs, les rôles, les fonctions et les relations entre eux qui interviennent dans le fonctionnement de l'entreprise. C'est principalement sur cette couche que va se porter ce travail.

Enfin, la couche application concerne, comme son nom l'indique, les considérations applicatives. Les articles [45], [29] et [31] par exemple, qui concernent

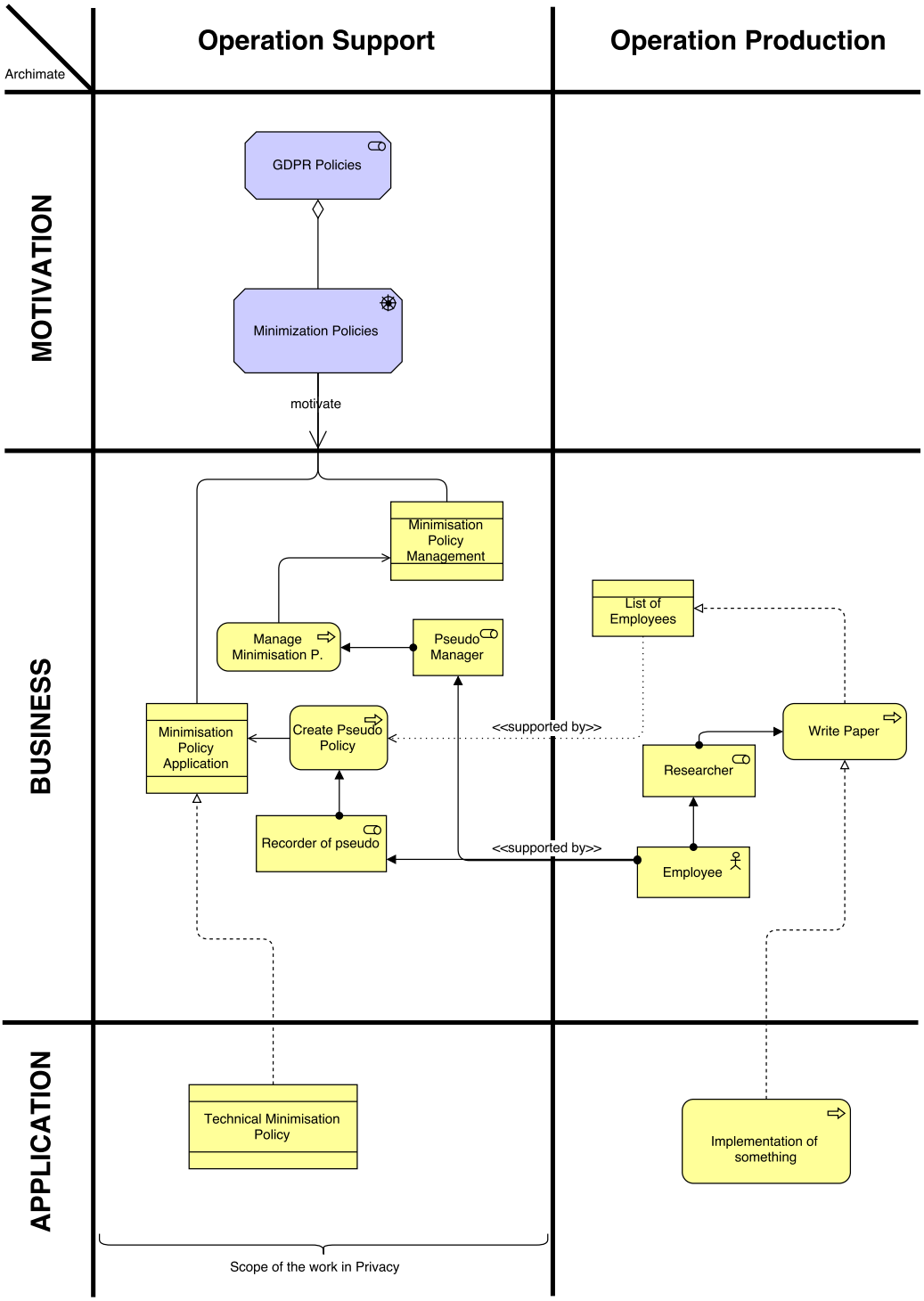

FIGURE 3.3 – Idée de l'instance du méta-modèle.

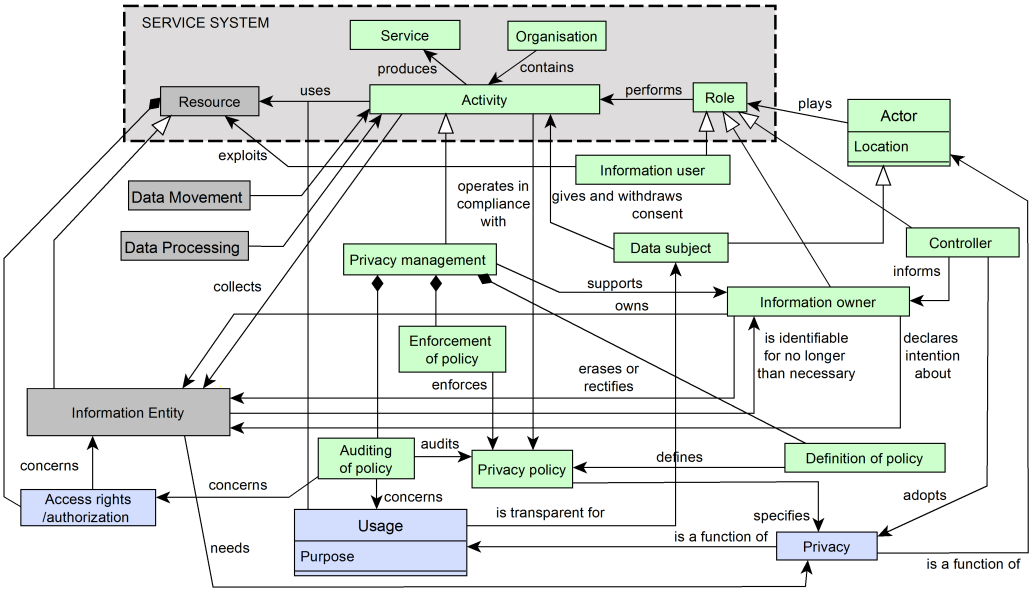

FIGURE 3.4 – Méta-modèle de Feltus et al. où la gestion de la vie privée est intégrée aux activités de l'entreprise.

des considérations de niveau plus applicatifs avec la k et la *l-anonymity* ; ou encore [39] qui présente une méthode de protection de la vie privée au niveau de la localisation des personnes, expriment des solutions à ce niveau.

Il peut exister des couches encore inférieures, comme la couche physique, mais elle ne sera que mentionnée car elle est hors du cadre de ce mémoire.

Le cadre de ce travail se trouve spécifiquement à l'**intersection des opérations de support et de la couche business**, avec une considération notable pour la couche motivation. Cette dernière reprend globalement les principes tels qu'ils seront présentés dans la section 3.

2.3 Spécialisation du premier méta-modèle

Suite à l'instanciation du méta-modèle, il est possible d'apporter une spécialisation de ce-dit méta-modèle. Cela est réalisé sous deux points de vue différents : un premier méta-modèle d'un point de vue inter-aspects et l'autre d'un point de vue inter-couches.

La première spécialisation (Figure 3.5) porte donc sur les aspects. Le premier méta-modèle a été dupliqué presque à l'identique mais en apportant une dimension transversale entre la production et le support via un lien nommé "support" entre les éléments d'un aspect à un autre.

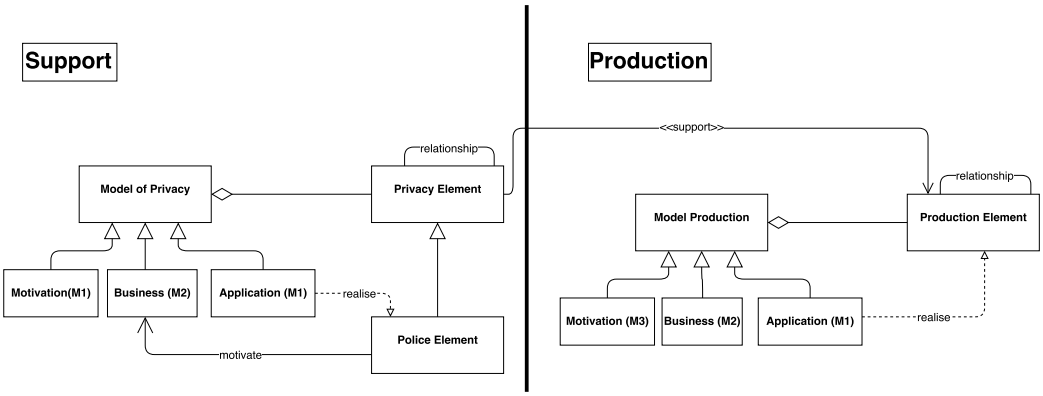

FIGURE 3.5 – Méta-modèle inter-aspects

La seconde spécialisation (Figure 3.6) concerne les relations entre les trois couches de niveau d'abstraction. Encore une fois, les couches pourraient être plus nombreuses mais on se limite ici à trois seulement. Dans ce modèle, le méta-modèle a été développé pour préciser chaque type d'élément. Un modèle de type motivation peut donc être composé d'éléments de motivation qui peuvent notamment être des éléments d'exigences. Ces derniers motivent donc des modèles de niveau management. Et ainsi de suite, de couche en couche. Tous les éléments sont des spécialisations d'un super-type "Element". Enfin, des vues supportent les polices de type business ou motivation.

3 Extraction de concepts légaux

Remarque préliminaire : Dans cette section, les termes "élément" ou "élément légal" sont utilisés pour exprimer le fragment de connaissance le plus atomique capable de porter une prescription légale (*Normative Proposition*) [43] comme cela a été décrit à la section 3 du chapitre 2.

Cette méthodologie s'emploie à créer non seulement un méta-modèle de vie privée, mais surtout à le faire suivant une législation particulière. Cette sous-section présente donc la manière d'extraire les concepts légaux d'un texte légal particulier. L'application de cette extraction du GDPR se trouve à la section 1 du chapitre 4.

Comme cela a été décrit dans l'état l'art, il existe plusieurs méthodes permettant d'extraire de manière systématique les exigences légales afin de les manipuler dans un cadre formel. Néanmoins, ces méthodes manquent de flexibilité et ne permettent pas une réflexion sur des grands principes d'un domaine, dans ce cas sur les principes de vie privée.

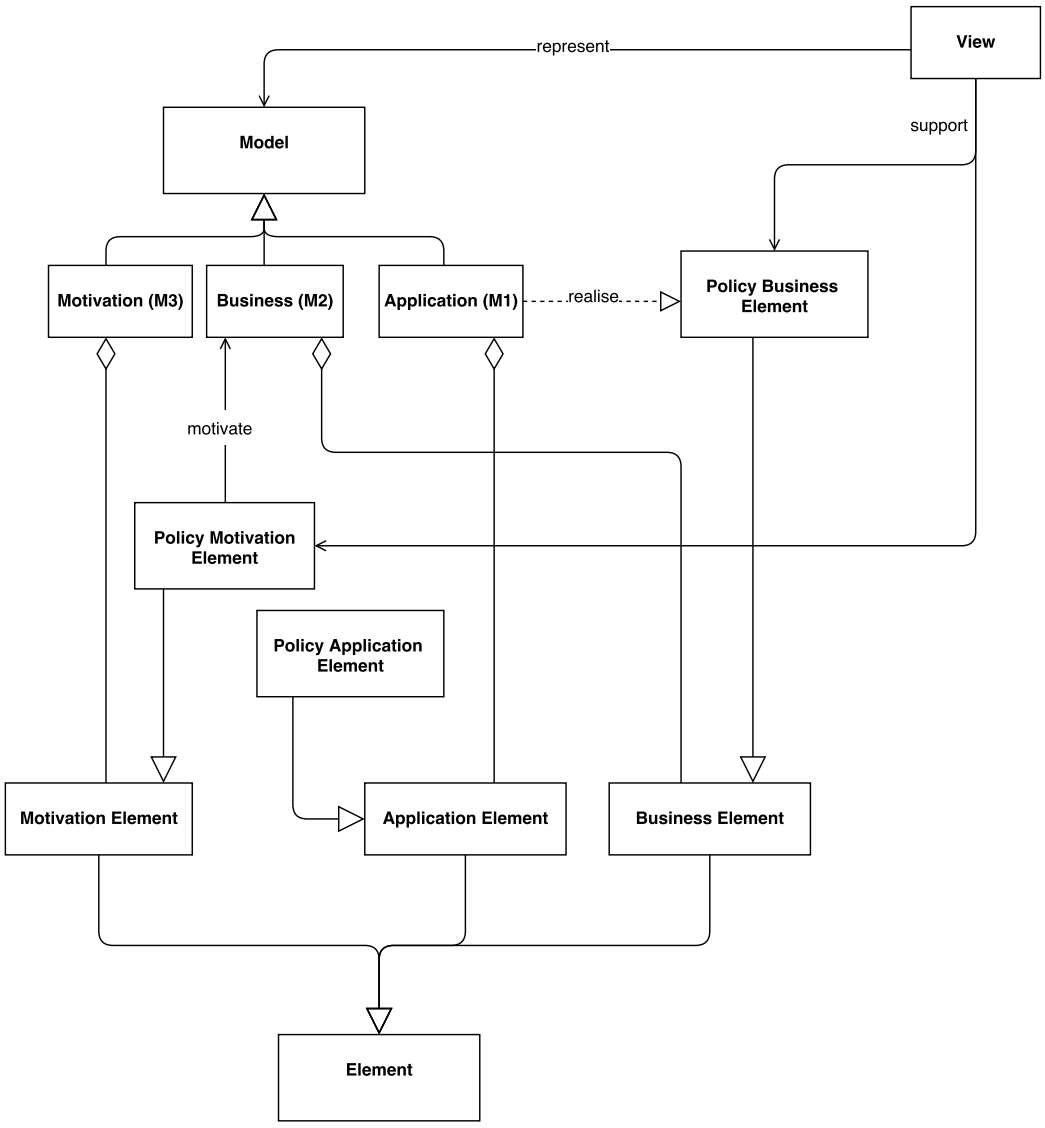

FIGURE 3.6 – Méta-modèle inter-couches

La méthodologie consiste ici donc à extraire les éléments par type, par thème, par domaine ou par éléments ayant la même considération. Dans le cas du GDPR qui est présenté dans la section 1 au chapitre 4, le guide Bird&Bird [7] a servi de base afin de déterminer une première approche d'extraction par thème. Durant ce processus, il convient de ne considérer qu'une partie des éléments suivant l'objectif poursuivi. Dans l'étude du GDPR présentée à la section 1 du chapitre 4, par exemple, seuls sont considérés les éléments ayant un impact direct sur le management d'une entreprise (entre autres, les actes délégués ne sont pas pris en compte).

Cette étape doit permettre d'aboutir à un ensemble de concepts avec un premier tri par thèmes. Chacun de ces éléments doit comporter une traçabilité avec l'article légal dont il est issu.

D'autre part, même si cela n'est pas absolument nécessaire, il peut être judicieux de créer un aperçu graphique de cette extraction ; l'analyse qui en découlera en sera d'autant plus aisée. Pour le cas du GDPR, un Mind-Map des éléments se trouve à la section 2 du chapitre 4.

4 Modélisation par principe

L'originalité de la méthodologie présentée ici est de proposer une manière de modéliser la vie privée basée sur les textes légaux, en ayant une vue **orientée principe**. Plus concrètement, cela signifie que le contenu des textes est analysé au regard de grands principes de vie privée, principes que l'on extrait d'une revue de la littérature scientifique et de standards. L'avantage de cette méthode est qu'elle permet d'avoir une validation grâce à ces articles scientifiques et les standards établis. La modélisation se fera donc par catégorie. Par exemple, dans la section 6 du chapitre 4 est présentée la modélisation du consentement. Ce consentement étant un grand principe de vie privée, la transformation du texte légal en un modèle conserve un certain lien avec la littérature scientifique.

4.1 Principes de vie privée

Une définition approximative et personnelle donnée aux termes "principes de vie privée" est la suivante : élément de contribution pertinente pour la réalisation de la vie privée.

Cette étape consiste donc à déterminer les principes qui régissent le domaine d'étude, la vie privée dans ce cas précis. Afin de réaliser cela, il est nécessaire de faire une revue de la littérature afin de faire une synthèse des auteurs donnant une liste et une description pertinente des principes. La

Figure 3.7 décrit un exemple de découpage des principes. Ce dernier met aussi en lumière le fait que certains concepts appartenant à d'autres principes peuvent également s'inscrire dans le principe étudié. Cet état de fait est intéressant car il montre que, lorsque plusieurs principes seront implémentés, il existera des interactions entre eux. Cela permettra d'affermir une double validation entre les éléments. Cette double validation est discutée à la section 5.

4.1.1 Synthèse de la revue de la littérature

Une fois que cette revue est terminée, il convient d'en extraire les principes présentés, de les compiler et de les synthétiser. Cette seconde étape se conclut donc par une synthèse des principes présentés par les divers auteurs.

Il ne reste plus qu'à sélectionner un principe, le modéliser, puis continuer ainsi jusqu'à obtenir tous les principes modélisés.

4.2 Modélisation

L'objectif est d'extraire les éléments légaux qui se rapportent au principe à modéliser, de les articuler entre eux et d'en créer un ou plusieurs modèles. Il existe des méthodes pour construire le modèle de manière systématique mais elles souffrent le plus souvent d'un manque de cohérence avec notre méthodologie orientée principe. En effet, les concepts légaux pour un principe sont souvent disséminés dans le texte légal et les relations entre eux peuvent être difficiles à établir de manière systématique ou semi-automatique grâce aux méthodologies analysées dans l'état de l'art.

Dans cette méthodologie, c'est le langage de modélisation ArchiMate [1] qui est utilisé. Ce dernier est intéressant puisqu'il offre des outils pour modéliser les aspects business, autant que les autres couches d'abstraction. C'est donc un outil intéressant pour ce modèle en 3 couches. Cela a déjà été discuté dans l'introduction.

La modélisation des concepts légaux peut être dérivée en un ou plusieurs modèles suivant l'utilité et le besoin. Par exemple, à la section 6 du chapitre 4, le principe de consentement est divisé en trois modèles inter-connectés : une partie statique, une partie fonctionnelle et une partie processus.

5 Discussion sur la double validation

L'intérêt de la méthode proposée dans ce mémoire repose sur le concept d'orienté-principe. A l'inverse des méthodologies de modélisation de textes

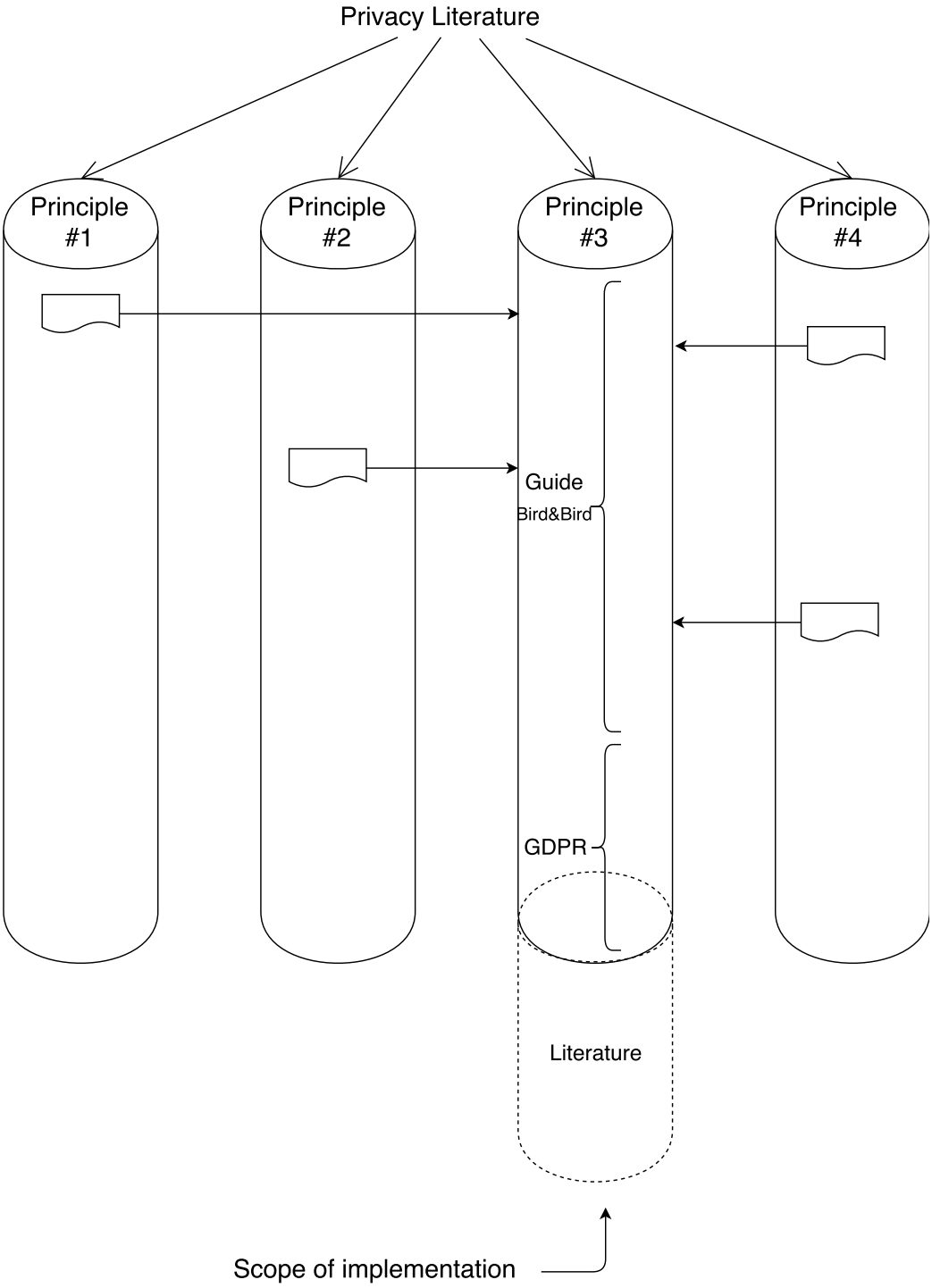

FIGURE 3.7 – Découpage par principes

légaux présentés dans l'état de l'art à la section 3 du chapitre 2, cette approche est moins systématique. En effet, pour modéliser un principe, une analyse transversale du texte légale est réalisée et les éléments légaux qui se rapportent à ce principe viennent de divers chapitres du texte. Lorsque cette méthode est appliquée principe par principe, il peut subsister des éléments légaux qui ne sont pas repris dans tous les principes réunis. Comme cela est montré dans la figure 3.8, l'intersection entre la couverture des principes peut donc être vide. Mais certains éléments légaux peuvent se retrouver dans plusieurs principes.

Par exemple, dans la section 3 du chapitre 4, parmi les principes identifiés se trouvent le consentement et la notification (et la transparence selon d'autres considérations discutées dans la section précitée). Pour obtenir le consentement éclairé d'une personne, il convient de lui donner un ensemble d'informations. Les deux principes se recouvrent donc sur ce point : il faut informer (principe de notification) la personne pour avoir son consentement (principe de consentement).

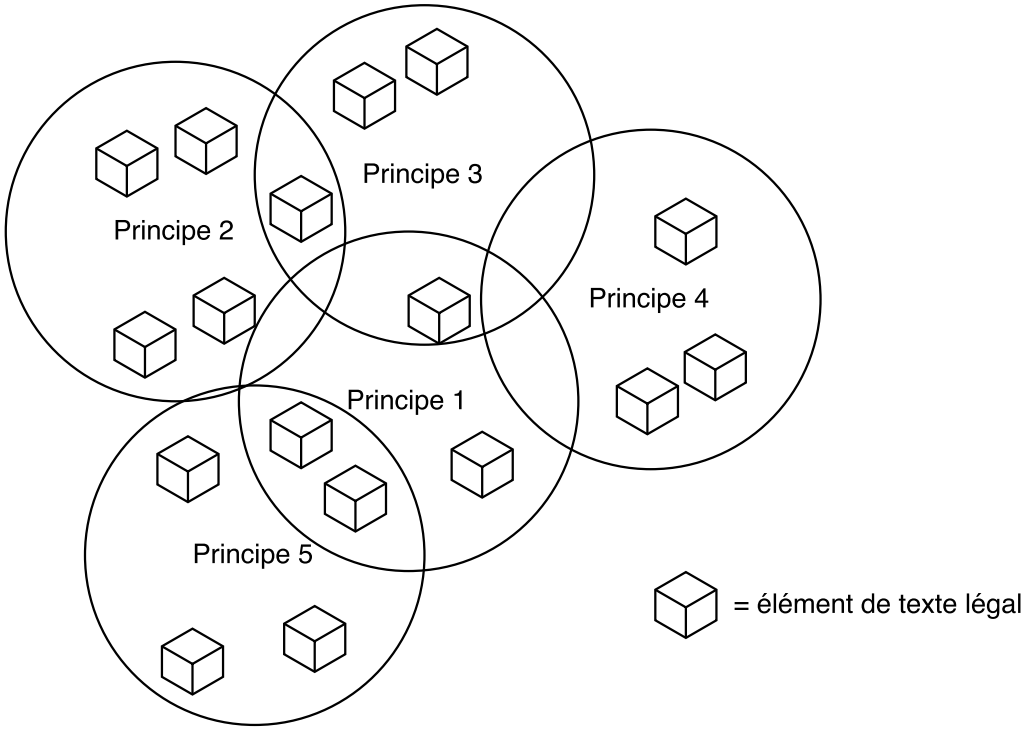

FIGURE 3.8 – Couverture des principes par rapport au texte légal

Grâce à ces intersections entre les principes et les emplacements des éléments, il est possible d'établir une cartographie de l'inscription du texte légal

dans les principes et donc valider les principes ; mais aussi de vérifier la couverture d'un texte légal sur ces principes et valider son étendue. En résumé :

- Les principes identifiés peuvent être validés en vérifiant leur présence dans le texte légal ;
- Et le texte légal peut être validé en vérifiant qu'il recouvre bien les principes donnés par les standards et la communauté scientifique.

6 Concepts transversaux à la méthodologie

Tout au long de la méthodologie présentée dans cette section, il convient de mettre en place certaines pratiques transversalement aux diverses étapes qui la composent. Cette section présente donc ces pratiques nécessaires à la bonne mise en place de cette méthodologie.

6.1 Traçabilité des articles

Lors de l'extraction des éléments légaux, il est nécessaire de garder une référence à ces éléments. Par exemple, un élément appartient à l'article 5, secondo, point a. Dans l'application au GDPR présente dans la suite de ce mémoire au chapitre 4, la notation suivante est utilisée : *Art. 5(2a)*.

Cette référence au texte légal doit apparaître à chaque étape de la méthodologie pour permettre d'avoir une traçabilité entre le modèle final et le texte légal d'origine.

6.2 Utilisation de framework

Comme cela a été présenté dans l'état de l'art, il existe plusieurs travaux qui présentent des frameworks de modélisation en conformité avec un document légal. Certains de ces frameworks pourraient avoir l'un ou l'autre aspect intéressant pour cette méthodologie. Dans ce mémoire, l'utilisation de l'un de ces frameworks a été évaluée : le *Legal-URN Framework for Legal Compliance of Business Processes* de Ghanavati [18]. Ce dernier a été choisi spécifiquement car il semble plus adapté à la problématique de ce mémoire : il pose la question de la conformité d'une entreprise d'un point de vue de la vie privée au niveau business.

Après une évaluation plus poussée, les résultats de cette évaluation ne sont pas convaincants pour trois raisons :

1. Le framework utilise un système d'arbre de goals (i*)[51]. Or, ce système n'est pas entièrement compatible avec une modélisation statique des données, notamment, et ne permet donc pas de ne modéliser

qu'une partie de l'objectif de la méthodologie présentée. La **sémantique** ne correspond donc pas à cette méthodologie.

Néanmoins, ce framework reprend, d'une certaine manière, le modèle en couche mis en place ici, ce qui lui donne tout de même un intérêt possible pour la modélisation des processus à l'intérieur du modèle qui est développé dans ce mémoire.

2. Ce framework travaille sur base de sections ou chapitres légaux, c'est-à-dire qu'il analyse une portion logiquement définie d'un texte légal pour ensuite établir un arbre de goals et ensuite des processus. Or, la méthodologie présentée ici repose en grande partie sur la vue transversale d'un concept à travers le texte. Ce framework n'est donc pas adapté en l'espèce. Sa **structure** ne correspond pas à la méthodologie.
3. Enfin, ce framework se concentre sur la conformité entre un cadre légal et des processus business existants pour une entreprise donnée. Or, cette méthodologie a pour objectif de justement obtenir un modèle générique de plus haut niveau adaptable à un grand nombre de systèmes. C'est donc la **finalité** qui n'est pas particulièrement adaptée à cette méthodologie.

Néanmoins, le framework pourrait être adapté afin de convenir à ce cas. Cela pourrait mériter un travail approfondi dans des travaux futurs.

Chapitre 4

Application à la GDPR

Dans le chapitre précédent, une méthodologie d'analyse de textes légaux et de modélisation de ces textes a été présentée. Afin de donner une première évaluation de sa validité, elle va être appliquée à un cas d'étude. Comme cela a été expliqué à la section 2 du chapitre 1, le cas d'étude présenté ici concerne le *Règlement général sur la protection des données* [2].

Au regard de la méthodologie, cette section sera articulée en plusieurs points : extraction des concepts légaux et articulation entre eux ; identification des principes de vie privée ; exploration et modélisation de deux de ces principes ; relations entre les modèles.

Acteurs

Cette section a pour objectif de présenter les 3 principaux acteurs concernés par le règlement et discuté dans ce chapitre.

La **personne concernée** est la personne identifiée ou identifiable grâce à une ou plusieurs donnée(s) la concernant. C'est-à-dire : toute personne pouvant être concernée par l'utilisation de ses données, typiquement un internaute.

Le **sous-traitant** est "la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement" [2]. Par exemple, ce sont les responsables informatiques d'une entreprise.

Le **responsable du traitement** est "la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement" [2]. Par exemple, ce sont les responsables business d'une entreprise.

1 Extraction des concepts légaux

Comme le GDPR est un texte long et qui comprend beaucoup de renvois d'articles, la première analyse et extraction des concepts légaux du document a été faite à l'aide d'un guide résumant et restructurant le contenu du règlement : *Guide to the General Data Protection Regulation*, par Bird&Bird [7]. Ce document permet d'aborder la régulation en donnant quelques balises d'aide à l'analyse.

Cette section suit la structure utilisée par Bird&Bird, en suivant point par point les titres du document.

La traçabilité des articles est mise en place grâce à un renvoi à la fin de chaque élément.

Il est à noter que certains des points qui suivent sont annotés comme "hors scope" puisqu'ils ne traitent pas du *core business* de la régulation. C'est-à-dire qu'ils concernent des éléments qui sont extérieurs à la mise en œuvre technique de cette régulation, comme par exemple : les amendes en cas de non-respect de la dite régulation ou l'obligation de collaboration avec les autorités en cas de problème.

1.1 Section 1 du guide : scope, calendrier et nouveaux concepts

1.1.1 Scope matériel et territorial

Le GDPR s'applique aux organisations établies en EU ayant des activités opérant sur des données à caractère personnel. Mais également à toute organisation non établie en EU mais offrant des services ou traitant des données à caractère personnel de citoyens de l'EU. Il existe des exclusions à ces règles, mais somme toute assez exceptionnelles, qui ne seront pas développées ici. Par exemple : la protection contre la criminalité par les autorités compétentes ou encore certaines institutions EU soumises à un autre régime.

1.1.2 Nouveaux concepts et concepts significativement modifiés

Note : Le guide aborde le texte légal en comparaison avec les anciennes directives européennes. Cela justifie les "nouveaux concepts [...] modifiés".

Ces éléments sont décrits plus en détails dans les points suivants du guide, ils ne seront pas abordés ici. A l'exception du terme "données personnelles/données sensibles" qui est définit comme : *données pour lesquelles un individu vivant est identifié ou identifiable, de manière directe ou indirecte.*

1.2 Section 2 du guide : Principes

1.2.1 Principes de protection des données

- Les données doivent être traitées de manière licite, juste et transparente ; art. 5(1a)
- Les données personnelles doivent être collectées pour des objectifs spécifiques, explicites et légitimes ; art. 5(1b)
- Minimisation des données : Les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire dans la réalisation de l'objectif ; art. 5(1c)
- Les données personnelles doivent être exactes et tenues à jour ; art. 5(1d)
- Limitation de stockage : les données personnelles ne doivent pas être conservées dans une forme qui permet l'identification des personnes concernées plus longtemps que nécessaire ; art. 5(1e)
- Intégrité et confidentialité : Les données personnelles doivent être traitées de manière à garantir leur sécurité : accès non autorisés, traitement illicite, perte accidentelle, destruction ou dommage ; art. 5(1f)
- Imputabilité : le responsable du traitement est responsable de montrer sa conformité à ces exigences. art. 5(2)

1.2.2 Licéité des traitements et des traitements supplémentaires

Conditions nécessaires à la licéité du traitement des données (au moins une doit être remplie) : (art. 6)

- Consentement de la personne concernée. (a)
- Le traitement doit être nécessaire à la réalisation d'un contrat ou préparer un contrat. (b)
- Le traitement doit être nécessaire à une obligation légale. (c)
- Le traitement doit être nécessaire à un intérêt vital pour la personne concernée. (d)
- Le traitement doit être nécessaire pour réaliser une tâche d'intérêt public ou d'une autorité officielle. (e)
- Le traitement doit être nécessaire à des buts d'intérêt légitime. (f)

1.2.3 Intérêts légitimes

Définition des intérêts légitimes : Les articles ne donnent pas de cas précis, mais les considérants donnent quelques exemples intéressants à considérer : (considérants 47 à 50).

Note lexicale : en droit, un considérant est défini comme : "chacun des alinéas d'un arrêt d'une cour et des décisions des juridictions administratives, qui commence par les mots *considérant que* et qui motive la décision". [1]

— Traitement pour du marketing direct ou pour la prévention de la fraude (47)
— Transmission de données à des buts d'administration interne (48)
— Assurance de la sécurité réseau et de l'information (49)
— Rapport de menace ou d'acte criminel (50)

1.2.4 Consentement

Le consentement d'une personne concernée est une indication spécifique, informée, non-ambigüe et donnée librement par le souhait de la personne concernée par lequel, par déclaration ou action affirmative claire, elle donne son accord pour traiter des données à caractère personnel qui la concernent.

— Le consentement au traitement contenu dans un écrit doit être distinguable des autres matières de la déclaration, intelligible, facilement accessible et dans un langage clair et simple. (art. 7(2))
— Les personnes concernées doivent avoir le droit de révoquer leur consentement à n'importe quel moment. Il doit être aussi facile de retirer son consentement que de le donner. (art. 7(3))
— Il est nécessaire de vérifier que les données recoltées sont toutes nécessaires à la réalisation du contrat (art. 7(4))
— Des traitements distincts doivent avoir des consentements distincts. (considérant 43)
— Pour les enfants, le consentement des parents doit être vérifié sous certaines dispositions particulières (voir le point sur les enfants). (art. 8)

1.2.5 Enfants

Le consentement des parents est nécessaire pour tout enfant ayant un âge en dessous de 13 ans et peut être demandé jusqu'à 16 ans. Chaque état membre décide de l'âge limite entre 13 et 15 ans (inclus). Art. 8

Les informations et communications adressées à des enfants doivent être dans un langage clair et simple qu'un enfant peut facilement comprendre.

1. `http://www.larousse.fr/dictionnaires/francais/consid\%C3\%A9rant/18384` ; Consulté le 18/05/2017

1.2.6 Données sensibles et traitement licite

Les données personnelles sensibles sont les suivantes : (art. 9(1))
- Origine raciale ou ethnique
- Opinions politiques
- Croyances religieuses et philosophiques
- Adhésion à un syndicat
- Données concernant la santé ou la vie sexuelle et l'orientation sexuelle
- Données génétiques
- Données biométriques utilisées dans le but d'identifier une personne On considère les photos comme des données sensibles si elles permettent l'identification ou l'authentification.

Il est interdit, sauf sous une des conditions ci-après, de traiter des données personnelles sensibles. Les conditions possibles sont les suivantes :
- Consentement explicite de la personne concernée ; art 9(2a)
- Nécessaire pour l'emploi, la sécurité sociale ou la protection sociale ; art 9(2b)
- Nécessaire pour protéger les intérêts vitaux d'une personne concernée qui est légalement ou physiquement incapable de donner son consentement ; art 9(2c)
- Dans le cas d'un groupement à but non lucratif (politique, religieux, syndical. . .), le traitement est autorisé uniquement pour les personnes concernées par le groupement ou les contacts proches ; art 9(2d)
- Données manifestement rendues publiques par la personne concernée ; art 9(2e)
- Nécessaire pour des raisons judiciaires ; art 9(2f)
- Nécessaire pour des raisons établies par le pays membre ; art 9(2g)
- Nécessaire pour des raisons liées à la santé ; art 9(2h)
- Nécessaire pour des raisons liées à la santé et d'intérêt public ; art 9(2i)
- Nécessaire pour des objectifs d'archives ; art 9(2j)

1.3 Section 3 du guide : droits individuels

1.3.1 Notifications d'information

Le responsable du traitement est obligé de fournir des informations aux personnes concernées sur le traitement de leurs données.

Les informations à fournir sont les suivantes :
- Identité et détails de contact du responsable du traitement, ainsi que ceux du Data Protection Officer ; art. 13(1a-b)

- Objectifs du traitement ; art. 13(1c)
- Destinataires ou groupes de destinataires ; art. 13(1e)
- Pour les données transférées hors de l'UE, leur moyen de protection et comment la personne concernée peut obtenir des infos sur les règles de transfert ; art. 13(1f)
- La période de rétention des données ; art. 13(2a)
- Les droits de la personne concernée sur : la rectification, la suppression et la restriction de ses données personnelles, l'opposition au traitement ainsi que le retrait de consentement ; art. 13(2b-c)
- Le droit de plainte de l'individu auprès de l'autorité de contrôle ; art. 13(2d)
- Les obligations pour le responsable du traitemeent de fournir les données, et les conséquences d'une non-exécution ; art. 13(1e)
- L'existence de décisions prises automatiquement ; art. 13(1f)

Ces informations sont à fournir : (art. 12(3))

- Au moment d'obtenir ces données s'il les obtient directement depuis la personne concernée ;
- Sinon :
  - dans une période de temps raisonnable, ou
  - dès qu'il y a communication avec la personne concernée, ou
  - avant que les données ne soient divulguées à un autre destinataire.

Le responsable du traitement doit également informer sur les types d'information traitée et leur source.

1.3.2 Accès, rectification et portabilité

Un individu a le droit de :

- Recevoir une confirmation que ses informations sont traitées ; art. 15(1)
- Accéder aux données (une copie) ; art. 15(3)
- Recevoir des infos supplémentaires sur le traitement :
  - L'objectif du traitement ; art. 15(1a)
  - Les types de données traitées ; art. 15(1b)
  - Les destinataires ; art. 15(1c)
  - La période de conservation ; art. 15(1d)
  - Le droit de rectification ou de suppression ; art. 15(1e-f)
  - La source des données ; art. 15(1g)
  - Les données traitées de manière automatique. art. 15(1h)

Et ce, sans retard excessif, dans un délai de maximum un mois.

La personne concernée peut demander au responsable du traitement de transférer ses informations à un autre responsable de traitement. Cela ne s'applique que à : (art. 20)

— Des données fournies par la personne concernée ;
— Des données traitées automatiquement ;
— Des données ayant un traitement autorisé par un consentement.

1.3.3 Droits de contestation

L'individu a le droit de contester :

— Le traitement à des fins de marketing direct ; art.21(1-2)
— Le traitement à des fins scientifiques/historiques/de recherche/statistiques ; art. 21(6)
— Le traitement pour les causes suivantes :
  — Intérêts légitimes ; ou art. 6(1f)
  — Pour des raisons d'intérêt public. Art. 6(1e)

Les individus doivent être notifiés de leurs droits de contestation.

1.3.4 Droit à la suppression et droit à la restriction de traitement

Les individus ont le droit d'avoir leurs informations effacées : art. 17(1)

— Quand les données ne sont plus nécessaires ; (a)
— Quand la personne concernée retire son consentement pour le traitement ; (b)
— Pour des raisons légitimes ; (c)
— Si les données seront traitées de manière illicites sinon ; (d)
— Si les données doivent être effacées pour être conformes à la législation. (e)

Le responsable du traitement obligé d'effacer des données doit informer tous les responsables de traitement qui ont accès à ces informations de les effacer également, dans la mesure du possible (les moyens de notification ne doivent pas être disproportionnés). Art.7 (2)

Les individus ont aussi le droit de restreindre les données, c'est-à-dire que le responsable du traitement peut seulement stocker les données. Ces restrictions sont applicables quand : (art. 18(1))

— Un individu conteste l'exactitude des données ; (a)
— Un individu conteste le traitement des données ; (b)
— Le traitement est illicite mais l'individu demande à conserver les données ; et (c)
— Le responsable du traitement n'a plus besoin des informations mais l'individu en a besoin pour des causes judiciaires. (d)

1.3.5 Profilage et prises de décision automatisées

Le profilage est défini comme : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. Art. 4(4)

Les restrictions sur les décisions basées uniquement sur les traitements automatisés (qui peuvent être du profilage) s'appliquent si le traitement produit des effets légaux ou des effets similaires. Ces traitements peuvent être utilisés si : Art. 22(1)

- Ils sont nécessaires au traitement d'un contrat entre le responsable du traitement et la personne concernée ; ou Art. 22(2a)
- Ils sont autorisés par l'UE ou l'état membre ; ou Art. 22(2b)
- Ils sont basés sur un consentement explicite de la personne concernée. Art. 22(2c)

La prise de décision automatique basée sur des données sensibles est plus restrictive, il faut : Art. 22(4)

- Le consentement explicite ;
- Ou une nécessité pour une raison d'intérêt publique substantiel.

1.4 Section 4 du guide : Imputabilité, sécurité et violation de sécurité

1.4.1 Obligations de data gouvernance

Le GDPR impose la *Privacy by Design* (Art. 25). Ces considérations sont hors du scope de ce travail puisqu'il concerne principalement des éléments de la couche applicative.

Le GDPR demande un PIA (*Privacy Impact Assessment*) pour chaque activité de traitement ayant un "risque élevé". Art 35

Les responsables du traitement et sous-traitants peuvent nommer un délégué à la protection des données et y sont obligés s'ils sont :

- Une autorité publique ; Art. 37(1a)
- Une organisation dont l'activité principale est le traitement automatisé de données personnelles ; Art. 37(1b)
- Obligés légalement par le pays membre. Art. 37(1c)

Les organisations de plus de 250 personnes doivent garder des enregistrements de toutes les activités de traitement. Avec notamment : Art. 30

- Nom et détails de contact du responsable du traitement (a)
- Les objectifs du traitement (b)
- La description des catégories de données (c)
- Les catégories de destinataires (d)
- Les transferts possibles (e)
- Les délais prévus pour la suppression (f) *
- Les mesures de sécurité techniques utilisées (g) *

Le caractère "*", utilisé au bout des deux derniers éléments, signifie que l'élément doit être mis en place "dans la mesure du possible".

1.4.2 Violation de données personnelles et notification

En cas d'incident tel que : une faille de sécurité entrainant la destruction, la perte, l'altération, la divulgation non autorisée accidentelle ou illicite de, ou l'accès à, des données personnelles transmises, stockées ou autrement traitées. Les obligations sont les suivantes :

- Le sous-traitant de notifier le responsable du traitement dès qu'il en a connaissance ; Art. 33(2)
- Le responsable du traitemeent de notifier l'autorité de contrôle, sans délai excessif et max 72h après l'avoir su. Si la faille ne risque pas de créer un risque pour les droits et libertés des personnes physiques, alors la notification n'est pas nécessaire ; Art. 33
- Obligation pour le responsable du traitement de communiquer une faille de sécurité aux personnes concernées sans délai excessif. La communication n'est pas nécessaire si : Art. 34
  - La faille ne présente pas de risque pour les droits et libertés des personnes concernées ; (b)
  - Des techniques de chiffrement éprouvées étaient en place ; (a)
  - Cela soulèverait des efforts disproportionnés. (c)

1.4.3 Codes de conduite et certifications

Le GDPR encourage la création de codes de conduite et de mécanisme de certification. Ces considérations ne seront pas abordées plus en détail dans ce mémoire.

1.5 Section 5 du guide : Transferts de données personnelles

Les transferts de données personnelles vers des pays tiers (extérieurs à l'UE) seront soumis à divers contraintes sur les destinations et les moyens de mise en œuvre, notamment à l'aide de codes de conduite et de mécanismes de certifications. (Art. 40 et 42)

1.6 Section 6 du guide : Régulateurs et mise en application

Cette section concerne la supervision des autorités ; leurs pouvoirs, responsabilité et tâches ; la coopération et la consistance entre le autorités de supervision ; et la création d'une autorité européenne de protection des données.

Ces éléments sont hors du périmètre de ce mémoire et ne seront donc pas considérés ici.

1.7 Section 7 du guide : Cas spéciaux : dérogations et conditions spéciales

Certains cas spéciaux imposent des restrictions de type : sécurité publique, sécurité nationale, défense, etc. D'autres provisions moins précises existent : liberté d'expression, accès public aux documents officiels, numéros d'identification nationale, obligation au secret, associations religieuses.

La recherche et les statistiques historiques et scientifiques sont une dérogation, à condition de ne plus pouvoir identifier les personnes (anonymisation ou pseudonymisation). Les mêmes conditions s'appliquent pour l'archivage avec un objectif d'intérêt public. Art. 89

1.8 Section 8 du guide : Actes délégués, actes implémentés et provisions finales

Cette dernière section précise quand le règlement entrera en vigueur et donne quelques provisions finales. Ces considérations ne sont pas très significatives pour l'objectif de ce mémoire.

1.9 Conclusion et discussion de l'extraction des concepts légaux

La première étape effectuée dans cette section a permis de mettre en évidence, en suivant la structure de Bird&Bird, les concepts importants du nouveau règlement de la privacy de l'Union Européenne. L'utilisation du guide a été utile pour plusieurs raisons :

- Une partie du travail de synthèse a été effectué ;
- Le document n'est pas rédigé en langage juridique et donc plus facile à aborder ;
- Les références sont souvent explicitées ce qui évite les recherches croisées à travers le texte légal.

Néanmoins, il souffre de défauts dans ce cas d'étude :

- Manque de précision : ce document est très pratique pour avoir une vue globale et un travail préliminaire afin d'entamer une lecture du GDPR. Mais, pour avoir une analyse plus complète, il est nécessaire de l'enrichir avec le texte légal original.
- Objectif du document : ce guide a pour objectif de montrer les évolutions et les différences par rapport aux régulations existantes. Cet objectif n'est pas commun avec celui de ce travail, le point de vue sur la question peut donc diverger légèrement.

Malgré ces éléments, et aux vues des points positifs, il semble que cette analyse soit assez satisfaisante pour être appliquée à la méthode présentée ici.

2 Articulation et classification des concepts entre eux

Il s'agit maintenant de reprendre les éléments extraits de la section précédente afin d'établir une première structuration ou articulation des concepts entre eux.

Pour ce faire, un outil de mindmaping a été utilisé. Le "Mind-map" permet de faire des liens entre une idée centrale et tous les éléments qui en découlent, construisant un arbre d'idées/concepts (un arbre au sens de la théorie des graphes). La figure 4.1 est un schéma qui décrit un découpage en Mind-map du GDPR. Cette structure offre un bon moyen de visualiser un grand nombre de concepts, avec une granularité pouvant être très poussée : une idée pouvant être affinée autant que souhaité.

L'inconvénient de cette méthode, de par la façon dont elle est utilisée dans le cadre de ce travail, est que la sémantique n'est pas toujours la même

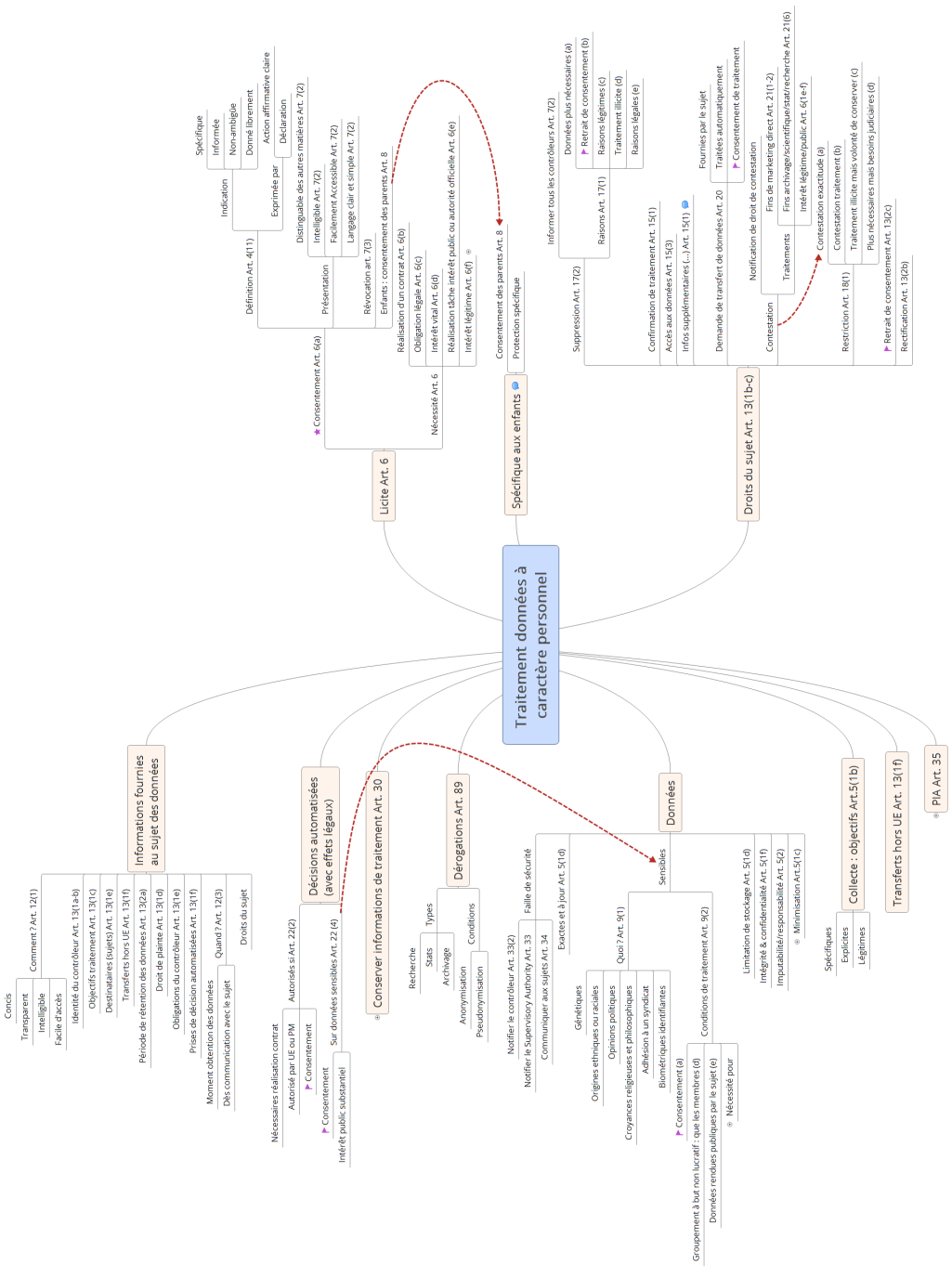

FIGURE 4.1 – Mind-map du GDPR

suivant les concepts. Par exemple, dans la figure 4.1, le traitement des données à caractère personnel a un lien direct à "licite", qui est une caractéristique, et un lien direct à "Données" qui est un sous-ensemble des considérations.

Ce schéma peut donc manquer d'uniformité, suite à ce problème de sémantique. Mais il possède l'avantage de pouvoir présenter tous les concepts — plus ou moins affinés — sur un seul schéma qui peut décrire potentiellement l'entièreté du GDPR.

Comme cela a déjà été discuté dans la méthodologie au chapitre 3, il est à noter que certains éléments du GDPR ne se trouvent pas dans ce Mind-map pour des raisons de délimitations du sujet. Par exemple, la partie concernant les amendes administratives ne se trouve pas dans ce schéma, puisqu'elle ne traite pas du *core business* du règlement.

Dans ce Mind-map, le concept central est "Traitement des données à caractères personnel". D'autres possibilités, ou vues, auraient pu être choisies comme GDPR, Data, etc. Cette décision a été motivée par deux choses :

1. Le guide Bird&Bird aborde le GDPR d'un point de vue plus orienté business que légal ;
2. L'objectif de ce travail concerne la couche business en particulier.

3 Identification des principes qui régissent la vie privée

L'objectif de cette section est de déterminer les principes de vie privée sur base de la littérature scientifique, comme cela a été défini dans la section 4 du chapitre 3.

Les sous-sections qui suivent présentent, pour chacun des auteurs, la liste des principes telles qu'ils les définissent.

Note : la traduction de l'anglais de certains principes peut perdre un peu de sémantique. Afin d'établir une traduction la plus consensuelle possible, l'article participatif de Pfitzmann et Hansen [40] a été utilisé dans ce travail, dans la mesure du possible. Par exemple, le mot le plus proche de "Accountability", sémantiquement et contextuellemment, est "imputabilité" qui, en français, est proche de "responsabilité". D'autres restent en anglais pour éviter une trop grande perte sémantique lors de la traduction.

3.1 GDPR : guide Bird & Bird

La deuxième partie du guide s'intitule *principles*, ce qui laisse supposer la définition des principes. Néanmoins, le sens ne s'entend pas comme étant

les principes de la vie privée, mais plutôt les principes du GDPR. Ceux-ci ne sont donc pas définis à un sens plus large pour la vie privée.

1. Licéité, transparence et *fairness*
2. *Purpose limitation*
3. Minimisation des données
4. Exactitude
5. Limitation de stockage : la forme de stockage ne doit pas permettre d'identifier la personne concernée plus longtemps que nécessaire
6. Intégrité et confidentialité
7. Imputabilité/responsabilité
8. Consentement
9. Nécessité
10. Enfants
11. Données sensibles

Dans les chapitres du guide qui suivent celui-ci, les éléments suivants sont cités : portabilité, notification et droits individuels. Ces derniers pourraient également faire partie de la liste de principes. Mais ils ne sont pas conservé dans cette liste, afin d'être le plus fidèle possible à l'analyse faite par le guide qui définit comme "principes", les éléments de la liste de onze éléments.

3.2 Privacy and Data Protection by Design

L'ENISA, la *European Union Agency for Network and Information Security*, a créé un document destiné à donner des indications sur la privacy par le design. L'ENISA étant un organisme reconnu dans le domaine, il est pertinent de se baser sur ces informations.

1. Léicité
2. Consentement
3. Objectif obligatoire
4. Nécessité et minimisation des données
5. Transparence et ouverture
6. Droits des individus
7. Sécurité de l'information
8. Imputabilité (accountability)
9. Protection des données par défaut et par design

3.3 Towards the development of privacy-aware systems

Cet article [24] cherche à créer une base de référence de systèmes privacy-aware et conformes aux régulations. Il met en évidence neuf principes de privacy établis par le conseil de l'Europe. Il fait ensuite la comparaison avec le système aux USA.

1. Traitement équitable et licite
2. Consentement
3. Spécification des objectifs
4. Minimisation
5. Divulgation minimale
6. Qualité de l'information
7. Contrôle de la personne concernée
8. Sensibilité
9. Sécurité de l'information

Un des principes n'est pas repris explicitement dans la liste, mais pourrait être ajouté à cette liste : l'information des droits de la personne concernée.

3.4 OECD Privacy Principles

L'OECD fournit un framework de privacy, fort utilisé, basé sur des lois de protection de la vie privée et proposant des principes et bonnes pratiques liées à la privacy. Ce qu'il propose est fortement lié aux législations présentes dans les pays membres de l'UE (Directive 95/46/EC).

1. Limitation de collection
2. Qualité des données
3. Spécification des objectifs
4. Limitation de l'utilisation
5. Garanties de sécurité
6. Ouverture
7. Participation individuelle : droit d'obtenir une confirmation
8. Imputabilité

3.5 Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems

Cet article [28] a été bien reçu dans par la communauté scientifique (nombre de citations important) et est donc une référence en la matière.

L'auteur, Langheinrich, présente tout d'abord de l'*US Privacy Act* de 1974 qui a été jugé insuffisant par l'OECD. Et il donne lui aussi une définition de ses principes de vie privée :

1. Notification : le principe d'ouverture ou simplement de notification
2. Choix et consentement
3. Anonymité et pseudonymat (traduction depuis [40])
4. Proximité et localité : la définition de l'auteur n'est pas claire
5. Sécurité adéquate
6. Accès et recours : la définition de l'auteur n'est pas claire

3.6 ISO29100

Le ISO/IEC 29100 :2011 [2] est une norme sur la vie privée.

1. Consentement et choix
2. Spécification et légitimité de l'objectif
3. Limitation de collection
4. Minimisation des données
5. Limitation d'utilisation, de rétention et de divulgation
6. Précision et qualité
7. Ouverture, transparence et notification
8. Participation individuelle et accès
9. Imputabilité
10. Sécurité de l'information
11. Conformité à la vie privée (semblable à l'imputabilité)

3.7 Tableau comparatif, analyse et discussion

La Figure 4.2 présente le tableau comparatif des principes.

La colonne de gauche reprend les auteurs/sources, la ligne du haut reprend les principes que l'on peut retrouver dans les différentes sources. Si une source

2. `https://www.iso.org/standard/45123.html`

Références/concepts	Rights of individuals	Consent	Portability	Openness	Notification	Limitations Minimisation/necessity	Limitations utilisation /purpose	Children	Privacy by Design	Lawfulness and fairness	Security	Accountability	Information Quality	Sensitive data
GDPR	Droit à l'oubli	Consentement	Portabilité des données	Droit d'information langage clair et simple	Droit d'information en cas de violation des données	Privacy comme norme	Limitation profilage	Protection spécifique	Privacy comme norme					
ENISA	Rights of the individual	Consent		Transparency and openness		Necessity and data minimisation	Purpose Binding / Necessity and data minimisation		Data protection by design and by default	Lawfulness	Information Security: Confidentiality, integrity, availability	Be able to demonstrate the compliance with privacy principles		
Towards the development of privacy-aware systems	Data Subject Control / +other statements	Consent	Minimal disclosure (to third parties)			Minimality	Purpose specification			Fair and lawful processing	Information Security		Information Quality : accurate, relevant, and complete	Sensitivity
OECD	Individual Participation Principle	~Collection Limitation Principle		Openness Principle		Collection Limitation Principle	Purpose Specification Principle / Data Quality Principle / Use Limitation Principle			~Collection Limitation Principle	Security Safeguards Principle	Accountability Principle	Data Quality Principle	
Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems		Choice and consent		Principle of Openness, or simply Notice	Principle of Openness, or simply Notice						Adequate Security			
ISO 29100	Individual participation and access	Consent and choice		Openness, transparency and notice	Openness, transparency and notice	Collection limitation / Data minimization	Purpose legitimacy and specification / Use, retention and disclosure limitation				Information Security	Accountability	Accuracy and quality	
TOTAL	4,5	5,5	2	5	3	5	5	1	2	2,5	5	3	3	1
Synthèse des définitions (de notre point de vue)	Droits de la personne concernée : retrait de consentement, effacement, rectification, contrôle des données, accès	Consentement actif, explicite, informé de l'intention de traitement des données	Portabilité à des acteurs tiers	Transparence : Permettre l'accès facile à l'information sur le traitement dans un langage simple et clair	Information en cas de violation, notification en cas de traitement, changement	Data minimisation : traiter le moins possible de données / seulement les données nécessaires	But : doit être nécessaire à la réalisation d'un contrat et bien défini / spécifique	Règles spécifiques à la protection des enfants	La privacy est prise en compte dès le design et est une fonctionnalité par défaut	Traitement et obtention des données doivent être licites	Traitement avec garanties de sécurité, protection contre les risques	Démontrer la conformité et contrôler le respect de la privacy, imputabilité.	Données doivent être exactes, pertinentes, à jour, adéquates et complètes en respect avec le but de leur collecte	Meilleure protection pour les données sensibles

FIGURE 4.2 – Tableau comparatif des principes de consentement

met en évidence un principe, une synthèse de quelques mots de sa définition est indiquée dans la colonne correspondante du tableau.

La ligne « Total » compte le nombre d'auteurs qui ont établi le concept comme étant un principe. Certains auteurs présentent un mélange de principes. Le caractère "∼" est dès lors présent dans la case correspondante. Cette case est alors considérée comme ayant une valeur de 0,5 au lieu de 1.

La dernière ligne donne une synthèse de chaque colonne, afin d'avoir une définition unique pour chaque principe donné. Cette définition peut ne pas reprendre tous les éléments de la colonne, puisque il y a une volonté de rendre la synthèse la plus consensuelle possible. Elle traduit également notre compréhension globale du principe.

3.7.1 Analyse et discussion

Tout d'abord, il est à noter que la frontière entre les différents principes n'est pas toujours claire et unanime. Selon les auteurs, les principes ne sont pas toujours exprimés sous le même terme ou la même forme. Certains principes sont fusionnés ; d'autres peuvent être distingués. Cela conduit à devoir prendre certaines décisions pour le classement des principes dans le tableau : par exemple, *Accountability* et *Privacy Compliance* ont été fusionnés et sont indistinguables dans le principe *Accountability*.

D'autre part, certains principes portent à confusion et peuvent être confondus suivant les auteurs :

- Minimisation des données/Limitation d'utilisation/Nécessité/Purpose : ces principes sont repris en 2 colonnes dans le tableau, mais on remarque que, selon les auteurs, ils peuvent être fusionnés, séparés, voire même repris plusieurs fois dans différents principes. Néanmoins, l'ISO29100 apporte une réponse pour trancher en disant que : "Data minimization is closely linked to the principle of *collection limitation* but goes further than that. Whereas *collection limitation* refers to limited data being collected in relation to the specified purpose, *data minimization* strictly minimizes the processing of PII." ; (en bleu dans le tableau)
- Openness/Notification : même problème avec une limite floue entre les principes (en orange dans le tableau).

Enfin, la ligne jaune en bas du tableau permet de déterminer quels sont les principes les plus cités par les auteurs. La suite de cette recherche va se porter sur un de ces principes.

Il est nécessaire de préciser que les sources du tableau ne sont peut-être pas exhaustives. Il pourrait exister d'autres auteurs ou standards définissant des principes de vie privée.

4 Exploration d'un principe : le consentement

Suite à la recherche sur les principes réalisée dans la section précédente, le principe de **consentement** va être exploré en particulier.

4.1 Motivation

La motivation de ce choix plutôt qu'un autre est déterminée par trois éléments :

1. Ce principe est l'un des plus cités dans la littérature ;
2. Le GDPR apporte une régulation plus stricte par rapport aux précédentes législations sur le sujet ; [7]
3. Le concept de consentement recouvre une grande partie d'autres concepts, ce qui ouvre à beaucoup d'opportunités de recherche et permet une double validation qui pourrait être satisfaisante.

Par ailleurs, les challenges qu'impose ce choix sont les suivants :

1. Le principe de consentement est assez complexe puisqu'il a des composantes transversales plus marquées que d'autres principes ;
2. Le consentement est un concept de haut niveau qui trouve aussi sa place, pour certains points, à un plus bas niveau, ce qui rend la définition de son impact compliqué.

4.2 Méthodologie de recherche du consentement

Afin de couvrir au mieux l'exploration du principe de consentement dans le texte légal, la méthodologie suivante est utilisée :

1. L'analyse extraite du guide Bird&Bird est d'abord utilisée. Le guide donne un point de vue global sur le GDPR et apporte donc un gain en terme de synthèse du principe pour le règlement ;
2. Pour compléter le guide, la recherche est étendue au GDPR lui-même. L'objectif étant d'avoir une analyse plus fine de quelques éléments qui peuvent manquer de précision ou de complétude ;
3. Enfin, pour enrichir au maximum le modèle, une revue de la littérature scientifique est réalisée. Cette revue permet d'apporter des éléments de motivation issus de la loi, de l'éthique ou de la philosophie par exemple, et donc d'affiner le modèle ; ou d'apporter des éléments de modélisation business faisant défaut dans le GDPR, qui est un texte purement légal.

La figure 3.7 montre cette structure (page 38).

4.3 Recherche dans le guide Bird&Bird

Cette sous-section présente les éléments directement extraits du guide. Ces éléments sont donc issus du GDPR mais c'est l'analyse faite précédemment qui est utilisée, donc celle issue du guide.

4.3.1 Définition large

Définition du consentement de la personne concernée : une indication spécifique, informée, non-ambiguë et donnée librement par le souhait de la personne concernée par lequel, par déclaration ou action affirmative claire, elle donne son accord pour traiter des données à caractère personnel qui le concernent.

Le consentement doit être explicite (Art. 4(11)) : cocher une case, choisir des paramètres techniques ou une quelconque déclaration qui indique clairement l'acceptation de la personne concernée. Le silence, des cases pré-cochées ou une inactivité ne constitue pas un consentement valide.

Un consentement est valide dans les conditions suivantes :

— Le consentement au traitement contenu dans une déclaration écrite produite par le responsable du traitement doit être distinguable des autres sujets dans cette déclaration, intelligible, facilement accessible et dans un langage clair et simple.
— Les personnes concernées doivent pouvoir révoquer (Art. 7(3)) leur consentement à tout moment, et ça doit être aussi facile de retirer son consentement que de le donner. En pratique, cela signifie que le retrait du consentement se fait sur le même média (par exemple : site, email, texte) que celui utilisé pour obtenir le consentement. Le retrait de consentement ne rend pas rétrospectivement le traitement illicite.
— Si le consentement est nécessaire à l'exécution d'un contrat, mais que ce consentement n'est pas nécessaire à l'exécution de ce contrat, il faut se poser la question de savoir si le consentement a été librement donné (Art. 7(4)).

Un consentement n'est pas considéré comme étant donné librement si :

— Il n'y a pas de provision pour séparer les consentements qui concernent des opérations de traitement différentes ; ou
— La réalisation d'un contrat est dépendante du consentement, malgré qu'un tel consentement ne soit pas nécessaire la réalisation de ce contrat.

4.3.2 Enfants

Des conditions spécifiques s'appliquent pour la validité du consentement donné par des enfants. Il est nécessaire d'obtenir et de vérifier le consentement des parents pour les enfants de moins de 16 ans (cette limite peut être descendue à 13 ans par les pays membres). Art 8

4.3.3 Recherche scientifique

Le consentement doit être obtenu pour des objectifs de recherche scientifique. Néanmoins, il n'est souvent pas possible d'identifier complètement les objectifs de traitement de données pour des objectifs de recherche scientifique au moment de la collecte des données. Il faut donc juste assurer que : (considérant 33)

- Les personnes concernées ont donné leur consentement pour certains domaines qui respectent les standards éthiques reconnus ; et que
- Les personnes concernées doivent être capables de donner leur consentement seulement pour certains domaines, ou des parties de projets de recherche dont l'ampleur est autorisée pour l'objectif prévu.

NB : le GDPR ne donne pas explicitement de détails sur l'obligation d'obtenir le consentement pour des objectifs de recherche scientifiques mais se réfère à des éléments généraux du droit. Néanmoins, on peut trouver les intentions dans les considérants 32, 33, 42 et 43.

4.4 Recherche via une exploration transversale

Dans la section précédente, tous les éléments qui apparaissent directement dans la section "consentement" du guide Bird&Bird ont été cités. Néanmoins, le principe de consentement se retrouve à divers endroits du GDPR, notamment sur son utilisation. Il est donc nécessaire de parcourir d'autres éléments afin d'avoir une recherche qui soit la plus exhaustive possible.

Deux pistes sont abordées ici :

1. Le guide, dans le chapitre sur le consentement, indique des informations supplémentaires présentes dans le chapitre sur les données sensibles et le traitement licite (section 4.4.1),
2. Le consentement est parfois intégré à d'autres prérogatives qui ne se basent pas sur le consentement, et se trouvent à d'autres endroits dans le GDPR. Afin de les identifier, le Mind-map réalisé précédemment sera utilisé (section 4.4.2).

4.4.1 Données sensibles et traitements licites

La personne concernée doit avoir donné son consentement explicite pour le traitement de données sensibles. Art 9(2a)

4.4.2 Analyse du Mindmap

On peut noter différents points où le consentement de la personne concernée est nécessaire :

- Dans le cas de décisions automatisées, il faut le consentement de la personne concernée et il doit être également explicite si le traitement porte sur des données sensibles ; Art. 22
- La personne concernée a un droit d'effacement (droit à l'oubli) si elle retire son consentement ; Art. 17(2)
- Si la personne concernée demande un portage de données (transfert de données) à un autre fournisseur, elle doit avoir déjà donné préalablement son consentement pour le traitement de ces données ; Art. 20
- Un traitement est licite uniquement si la personne concernée a donné son consentement ; Art. 6(a)
- La personne concernée doit être informée (information) par le responsable du traitement de son droit de retrait de consentement. Art. 13(2c)

4.5 Analyse de la CNIL

La CNIL[3] a fait une analyse minutieuse du GDPR et en a ressorti un graphe Dataviz faisant le lien entre les articles citants, cités et faisant références à des considérants. Dans cette analyse, ils ont également mis en avant plusieurs concepts qui ressortent tels que : les tranferts, la pseudonymisation, la certification... et d'autres. On y trouve notamment le concept de consentement. En suivant les liens reliés au consentement, il est donc possible de lister tous les articles et considérants qui y sont liés.

Les considérants n'apportant qu'un propos optionnel quant à la licéité, ils ne seront pas considérés.

Les articles, quant à eux, sont les suivants : 7, 8, 9, 13, 14, 17, 20, 22, 40, 49 et 83. L'analyse faite précédemment avait inclus les articles 4(11) et 6(1)a. L'article 83 concerne les conditions générales pour imposer des amendes administratives, ce qui est hors du cadre de ce travail. L'article 49 traite de

3. `https://www.cnil.fr/fr/reglement-europeen-protection-donnees/dataviz` Consulté le 18/05/17

dérogations dans des situations spécifiques et l'article 40 concerne les codes de conduites, ces points ne seront pas abordés afin de limiter le champ de recherche ; puisque ces éléments ne constituent pas le cœur du règlement.

La liste finale des articles qui concernent le consentement dans le GDPR est donc la suivante : 4, 6, 7, 8, 9, 13, 14, 17, 20 et 22.

4.6 Revue de la littérature scientifique

Ce dernier point d'exploration va présenter le consentement dans le contexte de travaux de divers auteurs dans la littérature scientifique. Les articles présentés ici ne se retrouvent pas nécessairement dans l'état de l'art puisque cette exploration vise à affiner les informations sur le consentement.

Cette liste n'est pas exhaustive, mais elle permet d'avoir un apport externe au modèle.

4.6.1 Projet EnCoRe

Le projet EnCoRe est un projet développé dans les labo HP afin de créer un framework de "privacy policies".

Parmi les articles qui ont été publiés durant le projet, l'un d'eux [33] présente une manière d'impliquer la personne concernée dans ses préférences de vie privée et en particulier de son consentement. Le point important de ce framework est que ces préférences peuvent être partagées entre plusieurs organisations.

D'un point de vue plus technique, un élément intéressant de ce framework est que le consentement et la révocation sont traités du côté client et non du côté serveur. Cela montre d'autant plus la volonté de mettre la personne concernée en maître de ses données.

Dans un second article de ce projet [50], les auteurs présentent certains fondements du consentement grâce à divers concepts tels que le contrôle, le but, l'information ou la révocation. Ils affirment que le consentement est probablement l'un des mécanismes les plus importants afin de déterminer "comment et quand les données peuvent être utilisées". Ils mettent aussi en évidence le besoin pour la personne concernée d'avoir un consentement éclairé. Tout en indiquant néanmoins que peu d'utilisateurs lisent et comprennent les notices de vie privée qui se présentent à eux.

Deux autres articles du projet [32] [38] mettent en évidence la nécessité d'attacher les données relatives à la vie privée aux données de la personne concernée.

4.6.2 From Privacy Promises to Privacy Management

Cet article [6] présente un framework afin d'attacher les données de vie privée –et notamment du consentement– aux données de la personne concernée. L'auteur appelle ça des "Sticky policies", c'est-à-dire des polices collantes, ce qui décrit bien l'idée.

4.6.3 Enhancing User Privacy through Data Handling Policies

L'auteur de cet article [5] met lui aussi en évidence que le consentement doit être lié aux données qui sont récoltées, et uniquement pour l'objectif énoncé.

Pour autant, il met aussi en exergue que ce n'est pas toujours facile à respecter, notamment pour les données de recherche. Il donne une solution possible en proposant de prévenir la personne concernée que les données peuvent être utilisées pour d'autres objectifs. Il propose également de garantir un contrôle continu à la personne concernée. Cela se rapproche de la proposition faite dans le projet EnCoRe à la sous-section 4.6.1.

4.6.4 Privacy Self-Management and the Consent Dilemma

L'article [44] présente des questions éthiques et philosophiques sur le consentement donné librement par une personne. Il pose la question : si la personne donne son consentement à quelque chose qu'elle ne comprend pas, son consentement n'est plus éclairé ; mais si le choix est pris à sa place –par une réglementation par exemple– son consentement n'est pas valide pour autant. Comment la personne peut-elle donc donner un consentement éclairé ?

Le consentement soulève donc des questionnements relatifs à la nature humaine même.

Même si cela n'apparaîtra pas dans le modèle développé ici, la réflexion est intéressante et il peut être intéressant d'en avoir un aperçu.

4.6.5 Informed Consent Online : a Conceptual Model and Design Principles

Ce dernier article met en place un modèle de consentement en ligne informé. Il se focalise d'abord sur 5 composants conceptuels : *disclosure*, *comprehension*, *voluntariness*, *competence* et *agreement*.

Il donne ensuite des principes de design afin de mettre en place le consentement informé, avec huit éléments à prendre en compte. Ces derniers prennent une approche orientée sur la balance nuisance/contrôle de l'utilisateur sur les demandes de consentement :

1. Décider si une aptitude est exempte de consentement informé ou non ;
2. Avoir une attention particulière lors de l'utilisation de l'approbation du consentement implicite pour des interactions web-based ;
3. Veiller aux valeurs par défaut ;
4. Donner le contrôle à l'utilisateur sur le « facteur de nuisance » ;
5. Éviter le jargon technique ;
6. Fournir les choix de l'utilisateur en termes d'effets potentiels plutôt qu'en termes de mécanismes techniques ;
7. Effectuer des essais sur le terrain pour aider à assurer des opportunités et une compréhension adéquate pour l'*agreement* ;
8. Avoir un design pro-actif pour le consentement informé.

4.7 Conclusion de la revue de la littérature

Les articles analysés apportent d'autres point de vue sur le consentement qui sont importants pour l'analsye avant de créer le modèle.

Ces articles apportent deux éléments intéressants : (1) une prise de distance pour avoir une vue plus globale, éthique ou de réflexion légale et (2) des structures de management et des frameworks.

Le premier point concerne donc une réflexion de plus haut niveau sur le consentement. Dans les articles sélectionnés, les auteurs portent souvent un regard de questionnement sur les fondements du consentement : la manière dont il est donné, son objectif, sa portée... etc. Mais également un historique ou des comparatifs avec d'autres organisations légales. Par exemple, l'article *Privacy Self-Management and the Consent Dilemma* compare les différences entre la législation américaine et européenne.

Le second point concerne des frameworks ou des structures de management du consentement dans le cadre de la privacy. Le projet EnCoRe apporte une importante contribution avec trois articles pertinents sur le sujet. L'inconvénient de ce qu'il propose réside dans le manque de limite entre les couches business et techniques. Cette limite manque souvent de clarté puisque ses modèles ne font pas de distinction de couches. Néanmoins, les différents articles sur le management du consentement vont permettre d'apporter des solutions business pour le modèle en construction.

Ce qui ressort de cette analyse est la distinction avec le GDPR. Ce dernier répond à un besoin législatif et impose donc, au-delà du design, des motivations de haut niveau de privacy. Alors que pour les articles, si certains donnent une réflexion de fond, d'autres cherchent à mettre en place des mécanismes pour répondre à ces besoins de plus haut niveau.

5 Le langage Archimate

En préambule de la modélisation, il convient de présenter brièvement les outils de Archimate utilisés dans la suite.

Une première approche sur la structure d'Archimate a été présentée à la section 4 du chapitre 1.

La figure 4.3 présente les éléments d'Archimate 3.0 utilisé dans les modèles. Les définitions sont extraites des spécifications du langage. [4]

Dans ce travail, la notion de "réalisation" est importante, elle représente la mise en oeuvre des exigences/motivations exprimées dans les textes légaux. De manière plus générale, cette relation représente la mise en oeuvres d'éléments d'une couche à un élément d'une couche supérieure, c'est la relation inverse de la relation "motive" définie dans le méta-modèle (section 2 du chapitre 3).

L'élément "contract" présente également une notion importante. Il est considéré ici comme le raffinement d'un principe, traduit en exigences représentées par un contrat.

6 Modélisation du principe de consentement

Le modèle de consentement est construit en plusieurs étapes. La première étape consiste à articuler les concepts entre eux et de comprendre leurs interactions. Ensuite, ces concepts vont motiver la création de trois modèles : le premier concerne les valeurs statiques, modélisé dans une structure passive ; le second et le troisième sont interconnectés puisque l'un correspond aux processus tandis que l'autre correspond aux fonctions.

Dans ArchiMate, les processus sont composés d'un ensemble d'étapes qui sont reprises dans les fonctions. Les processus peuvent être vus comme horizontaux et les fonctions comme verticales. Le schéma 4.4 décrit mieux cela.

Par exemple, dans un hôpital, on suppose la fonction "Accueil". Les processus "patient venant pour une consultation" ou "visiteur de malade" passent tous les deux par la fonction "Accueil", même si ce n'est pas pour le même objectif.

6.1 Articulation des concepts de consentement

Grâce à l'extraction faite précédemment dans la méthodologie, l'articulation des concepts entre eux peut être réalisée. Cette tâche n'est pas très

4. http://pubs.opengroup.org/architecture/archimate3-doc/

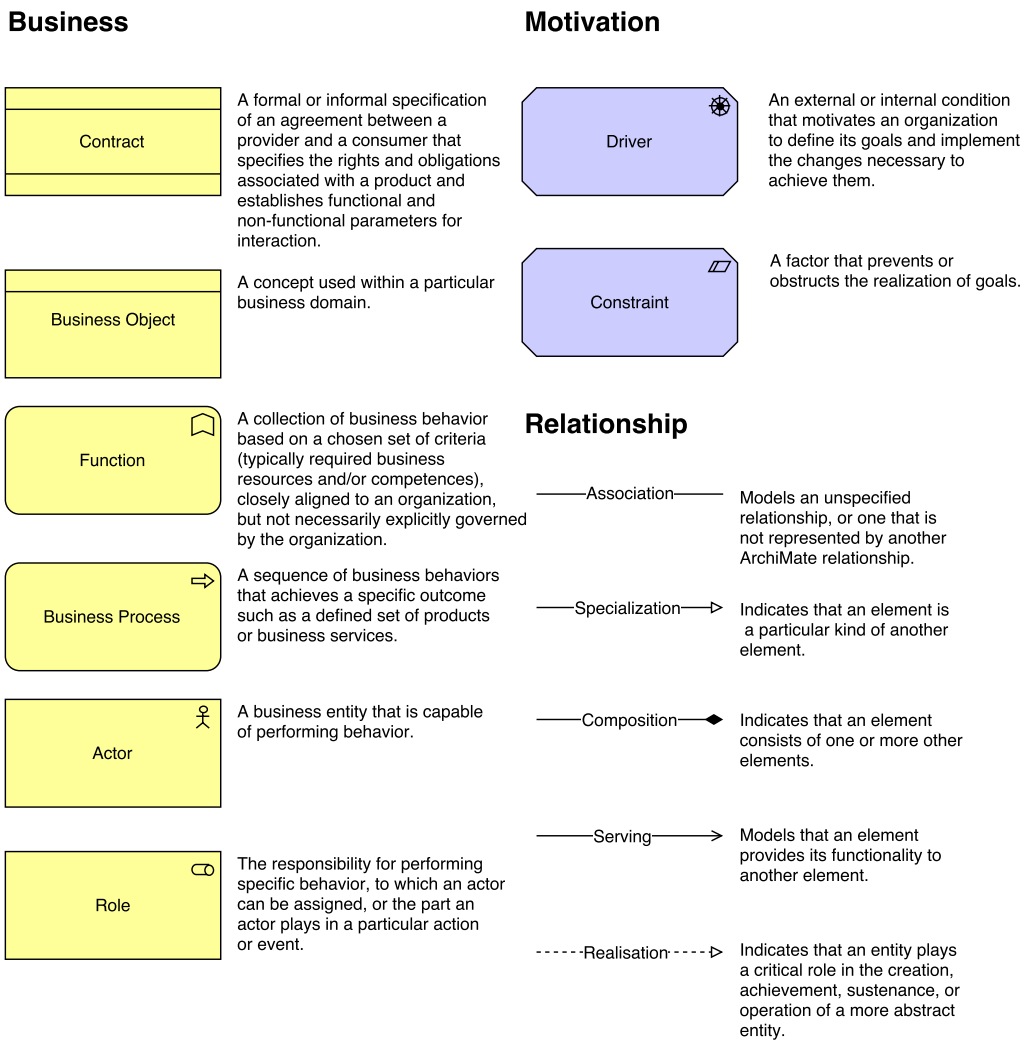

FIGURE 4.3 – Brève présentation d'éléments d'Archimate 3.0

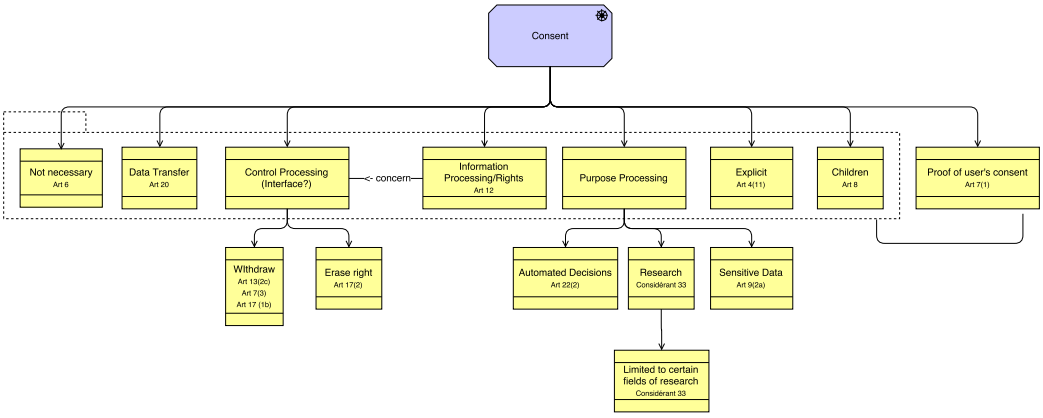

FIGURE 4.4 – Articulation des concepts de consentement

formalisée, mais sous l'éclairage (1) de la revue de la littérature, (2) de la sémantique des concepts et (3) du texte légal, il est relativement aisé de le construire.

La figure 4.4 présente donc les concepts qui ont été mis en évidence dans les étapes précédentes : le transfert de données, le retrait de consentement, le droit de suppression, les informations sur le traitement et les droits de la personne concernée, les objectifs de traitement (de type recherche, données sensibles ou traitement avec décisions automatisées ayant un impact juridique), le caractère explicite du consentement, les cas particuliers qui s'appliquent aux enfants et l'obligation pour le responsable du traitement de pouvoir prouver le consentement de la personne concernée.

Afin d'avoir une construction cohérente, voici les apports faits sur les relations entre les concepts :

— Le retrait et la suppression se retrouvent sous un concept de contrôle du traitement ;
— Les décisions automatisées, la recherche et les données sensibles se retrouvent logiquement sous le concept "Objectif de traitement" ;
— Enfin, la preuve du consentement concerne tous les autres concepts de consentement.

6.2 Structure passive

Le modèle passif (Figure 4.5) représente une traduction presque directe des éléments passifs du GDPR vers un modèle des objets business, avec certaines adaptations techniques explicitées dans la suite. En suivant le méta-modèle présenté à la section 2.3, au niveau motivation se trouve les *Children*

Policies (les règles qui concernent les enfants) ainsi que le *Purpose Processing* (l'objectif de traitement). Ces deux éléments sont hérités de l'articulation des concepts à la section 6.1.

Le *Purpose Processing* peut être spécialisé en différents types : données sensibles, recherches (lui-même pouvant être spécialisé) et décisions automatisées (lui aussi peut être spécialisé). Chacune de ces spécialisations requiert un consentement explicite pour le traitement des données de la part de la personne concernée. C'est-à-dire que pour chaque traitement d'un de ces types, un consentement explicite de la personne concernée est nécessaire.

Les données de la personne concernée sont une composition de deux choses : d'une part les données business, c'est-à-dire les données qui servent à réaliser la production, et d'autre part, les données de consentement au traitement. Par exemple, supposons une entreprise qui collecte le nom, l'adresse e-mail et la position des utilisateurs, cela concerne des données business. Si l'entreprise veut appliquer un traitement à ces données, elle doit obtenir le consentement de la personne concernée, qui fait donc aussi partie des données concernant la personne concernée. Il existe également un lien entre un consentement de traitement et un type de données en particulier [6].

Dans le cas des enfants, il est nécessaire que l'exigence soit réalisée par le consentement spécifique à l'enfant.

Enfin, pour certains traitements, dans le cas d'une autre nécessité (art. 6), le consentement n'est pas nécessaire.

6.3 Processus de consentement et modèle de fonctions

Les deux modèles qui suivent sont fortement corrélés et c'est la raison pour laquelle ils vont être discutés ensemble. En effet, dans le langage ArchiMate, une fonction représente un ensemble de capacités qui sont utilisées par des processus. Un processus va utiliser divers éléments proposés par des fonctions afin d'établir les étapes de son fonctionnement. La définition donnée par Archimate 3.0 est : "*A business function is a collection of business behavior based on a chosen set of criteria (typically required business resources and/or competences), closely aligned to an organization, but not necessarily explicitly governed by the organization.*" Un exemple est décrit au début de cette section.

En ce qui concerne le modèle de processus, trois sous-modèles décrivant trois processus différents relatifs au consentement ont été modélisés. Le processus le plus important ici est celui dédié à l'obtention du consentement.

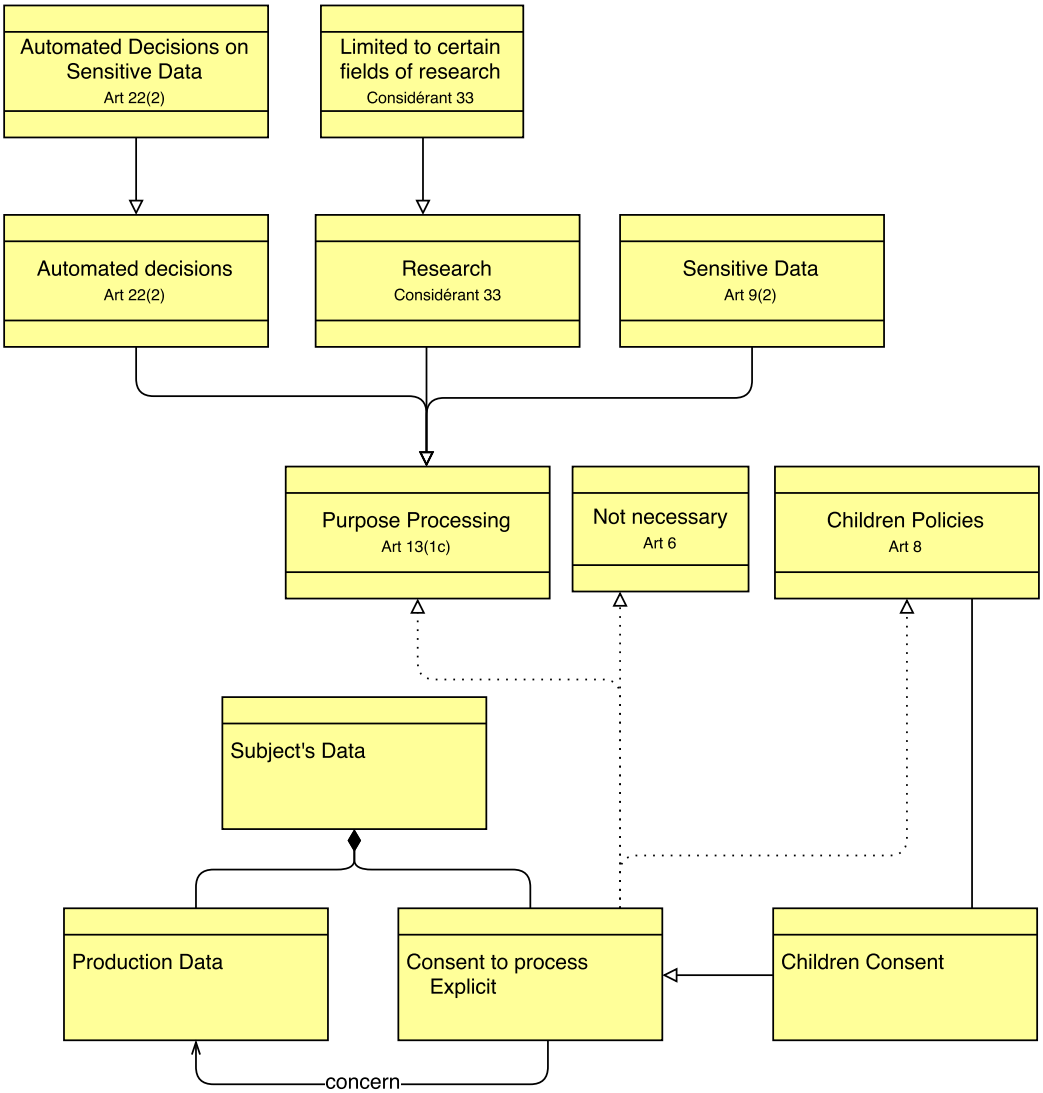

FIGURE 4.5 – Structure passive des données

6.3.1 Discussion sur le processus d'obtention du consentement

Afin de créer le modèle, le GDPR a été utilisé comme cadre légal. Néanmoins, pour modéliser un processus complet, la législation à elle seule ne suffit pas. C'est pourquoi une veille sur les processus de consentement a été réalisée afin de déterminer un processus existant pouvant convenir à ce modèle. Cette veille se trouve en annexe A.

Le processus retenu est celui de l'ACRP ou *Association of Clinical Research Professional*, qui est une association basée à Washington qui travaille sur la recherche clinique. Ils ont écrit un *White Paper* sur le processus du consentement informé dans ce contexte.

Le processus qu'ils proposent pour obtenir le consentement est le suivant :

1. Assurer que l'environnement convient.
2. Assurer que la personne a la capacité de consentir, c'est-à-dire la capacité cognitive et légale de fournir un consentement informé.
3. Les éléments du consentement doivent être présentés et discutés avec la personne concernée d'une manière séquentielle. Il est également conseillé de poser des questions ouvertes à la personne concernée pour vérifier sa compréhension.
4. Le temps entre la présentation des éléments et le consentement peut être plus ou moins grand suivant la nature des éléments. Dans le cas de consentement portant sur un élément important ou risqué, une procédure de consentement décalé peut être envisagée pour laisser le temps à la personne concernée de réfléchir à son consentement.
5. Assurer la compréhension de la personne concernée. Une méthode possible est de proposer un test avec des questions à choix multiples afin d'évaluer la compréhension de la personne concernée.
6. Documenter le consentement informé
7. Redemander le consentement de la personne concernée au cours du temps, en cas de modification ou après une longue période.

Étant donné que ce processus a été mis en place dans un cadre médical, il est nécessaire d'y apporter quelques adaptations pour qu'il soit conforme à un champ plus large que celui de la santé.

Dans la liste qui suit sont décrites point par point les adaptations effectuées sur le processus, de même que les points de jonction.

1. **Environnement :** Il convient d'obtenir le consentement dans un lieu et un moment approprié donc privé, confidentiel et sécurisé pour la personne concernée, comme un cabinet médical. Il s'agit donc de déterminer de quelle manière on comprend l'environnement dans le cas de la vie privée en général :

— Soit c'est le **contexte** dans lequel se trouve la personne concernée. Cela prend donc en compte un grand nombre de facteurs comme le moment, le lieu, les personnes qui accompagnent ou entourent la personne concernée... etc. Or, dans le cadre de la vie privée, il est courant que la personne soit seule face à son ordinateur, et non pas face à un professionnel de la santé.
— Soit c'est la manière dont va être **sécurisé** –d'un point de vue des systèmes d'information– la manière d'obtention le consentement ; puisque l'objectif de cette étape est d'établir un espace privé, confidentiel et sûr.

Dans le cadre de ce travail, la deuxième option a été choisie (la sécurité) puisqu'elle parait plus proche de la réalité.

2. **Évaluer la capacité à consentir :** Il est nécessaire d'évaluer la capacité cognitive à consentir. Le GDPR ne donne pas de précision sur ce sujet, mais donne une grande importance aux enfants. Dans le cadre de ce travail, il est considéré que le responsable du traitement doit vérifier l'âge de la personne concernée, afin de vérifier s'il a plus ou moins de 16 ans (peut être descendu à 13 ans suivant les législations propres aux pays membres).
3. **Présenter les éléments du consentement :** Le guide décrit la manière dont les informations doivent être fournies à la personne concernée. Dans le cadre de ce travail, il convient de se concentrer principalement sur celles qui doivent être fournies. La manière avec laquelle elles doivent être exprimées est décrite dans le GDPR (intelligible, distinguable des autres matières... Art. 7) et la modélisation de cette forme sort du cadre de ce travail. Le guide met également en garde contre certains effets propres à la recherche scientifique ; dans ce contexte, cela ne concerne pas l'objectif de ce travail non plus.
4. **Utiliser une procédure de consentement décalé :** Le temps attribué afin de donner son accord pour un consentement peut être décalé entre la réception des informations et le-dit accord. Ceci afin de permettre à la personne concernée de réfléchir plus longuement, notamment sur des questions sensibles. Dans ce cas, ce point n'est pas mis en évidence à l'intérieur du modèle, mais peut être envisagé. D'autre part, le cas où surviendraient des questions suffisamment sensibles que pour nécessiter un temps de réflexion semble incompatible avec la réalité, si l'on considère des systèmes d'informations en ligne et en temps réel par exemple.
5. **Assurer la compréhension de la personne concernée :** Le GDPR ne stipule rien à ce sujet mais il semble judicieux de l'ajouter au proces-

sus afin de le rendre le plus robuste possible. Une solution envisageable est celle indiquée dans le guide lui-même : utiliser des questionnaires à choix multiples afin d'assurer la compréhension de la personne concernée.

6. **Documenter le consentement :** Le guide indique des préoccupations propres au milieu médical, ou tout du moins à une relation directe entre deux personnes physiques afin d'établir une preuve du consentement. Dans le cadre de ce travail, le fait d'enregistrer une preuve de consentement sous une forme papier signée, ou électronique avec un système éprouvé est considéré comme garantissant l'authentification et l'authenticité (signature électronique).
7. **Consentement continu :** Dans le milieu médical, il est nécessaire de faire un suivi sur le consentement de la personne concernée, afin de s'assurer qu'il est toujours éclairé. Dans le cas de ce travail, cela peut être considéré comme concernant d'autres processus : retrait de consentement ou modification des objectifs de traitement par exemple.

Remarque : Le guide indique qu'il ne prend pas explicitement les enfants en compte dans le processus et que ces derniers doivent faire l'objet d'un traitement particulier. Dans le GDPR, la considération du consentement des enfants a une place importante. Le modèle construit dans cette section possède un processus annexe qui, tout comme le guide l'indique, mériterait un traitement différent. Néanmoins, il ne sera pas abordé plus en détail dans le cadre de ce travail.

6.3.2 Remarque préliminaire relative à la lecture des modèles

Dans les modèles qui suivent, les éléments possédant un astérisque(*) sont ceux issus du guide sur les processus et ajoutés afin de conserver la cohérence du modèle. Les autres possèdent un ou plusieurs numéro(s) d'article(s) afin d'assurer leur traçabilité.

D'autre part, une définition propre a été établie pour les termes "Contrat de consentement". En effet, lorsque le consentement d'une personne concernée est demandé, il y a un ensemble d'informations à fournir afin que ce consentement soit éclairé. Ceci se rapporte au besoin de transparence mis en évidence dans le GDPR (considérants 39, 58 et 60). Dans le cadre de ce travail, le "contrat de consentement" représente l'ensemble des informations fournies par le responsable du traitement à destination de la personne concernée afin que cette dernière puisse rendre un consentement éclairé, suivant les exigences du GDPR.

Parmi les informations, il en existe une qui dit que le responsable du traitement doit stipuler l'objectif du traitement (Art. 13(1c) et Art. 6) ainsi que la base légale sur laquelle elle repose. Cette dernière est vraisemblablement celle indiquée à l'article 6(1b) : c'est-à-dire nécessaire à l'exécution du contrat. La personne concernée donne son consentement pour le traitement avec un objectif donné. Il est donc nécessaire de stipuler explicitement cet élément dans le modèle de processus.

6.3.3 Description des modèles de processus

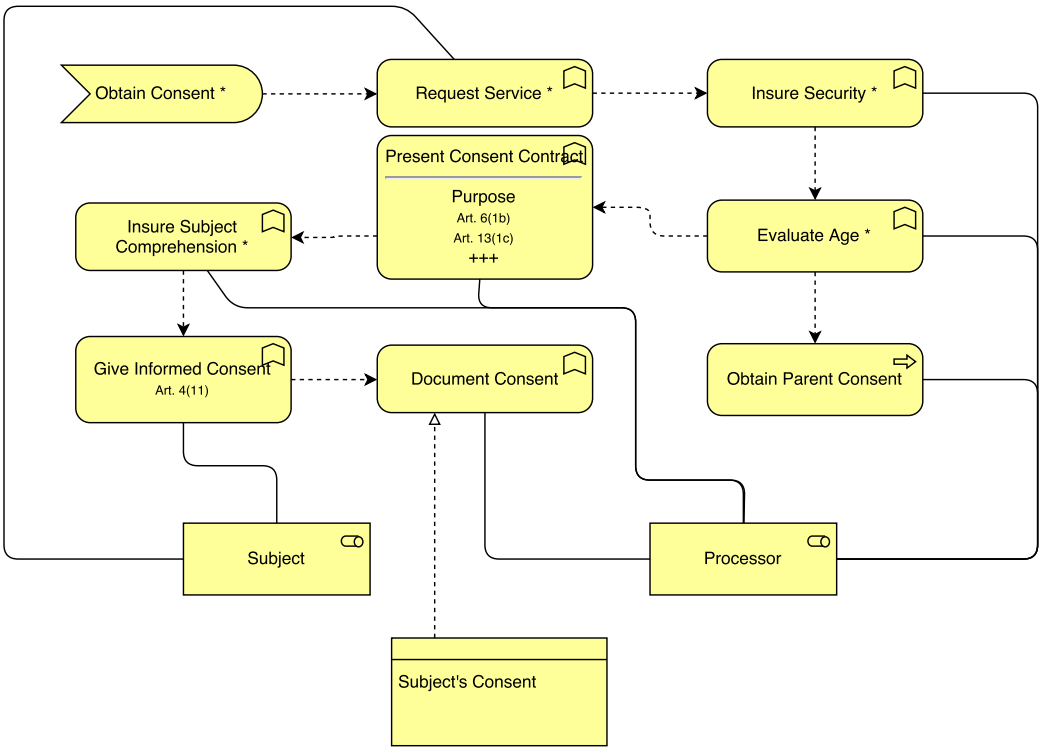

FIGURE 4.6 – Modèle de processus d'obtention du consentement

Obtention du consentement Comme déjà décrit précédemment, le processus suit le guide de conduite de l'ACRP moyennant quelques adaptations pour être plus conforme à la vie privée. La figure 4.6 représente ce modèle.

Tout d'abord, il y a un évènement qui peut venir du sous-traitant ou de la personne concernée qui déclenche la nécessité d'un consentement pour un service auprès de la personne concernée. Le sous-traitant commence par assurer une communication et un stockage sécurisé qui assure la confidentialité, l'intégrité et la sûreté. Ensuite, il doit faire une évaluation de l'âge. Dans le

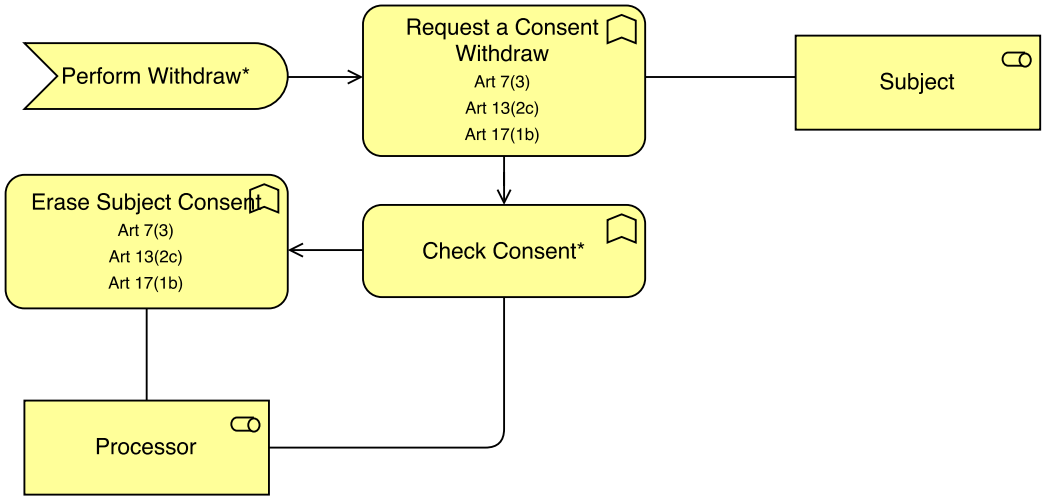

FIGURE 4.7 – Modèle de processus de retrait de consentement

cas où la personne a moins de 16 ans (valeur sujette à variations suivant le pays membre (Art. 8)), un processus d'obtention du consentement des parents doit être mis en œuvre. Dans le cas contraire, le sous-traitant présente les conditions du contrat de consentement (section 6.3.2). Le responsable du traitement doit également assurer la compréhension de la personne concernée ; une suite de question à choix multiples est généralement une bonne méthode [34]. Lorsque tout cela a été fait, la personne concernée peut donner ou non son consentement, que le sous-traitant documente.

Réaliser un retrait de consentement Ce modèle est représenté à la figure 4.7.

La personne concernée demande à retirer son consentement. Le sous-traitant vérifie l'existence du consentement et le supprime. Les traitements qui dépendaient de ce consentement deviennent donc prohibés.

Réaliser un transfert de données Ce modèle est représenté à la figure 4.8.

La personne concernée demande à transférer ses données chez un autre responsable de traitement. Le sous-traitant vérifie donc l'existence du consentement qui concerne le traitement des données en question et les transfère à l'autre sous-traitant, ainsi que le consentement qui y est lié.

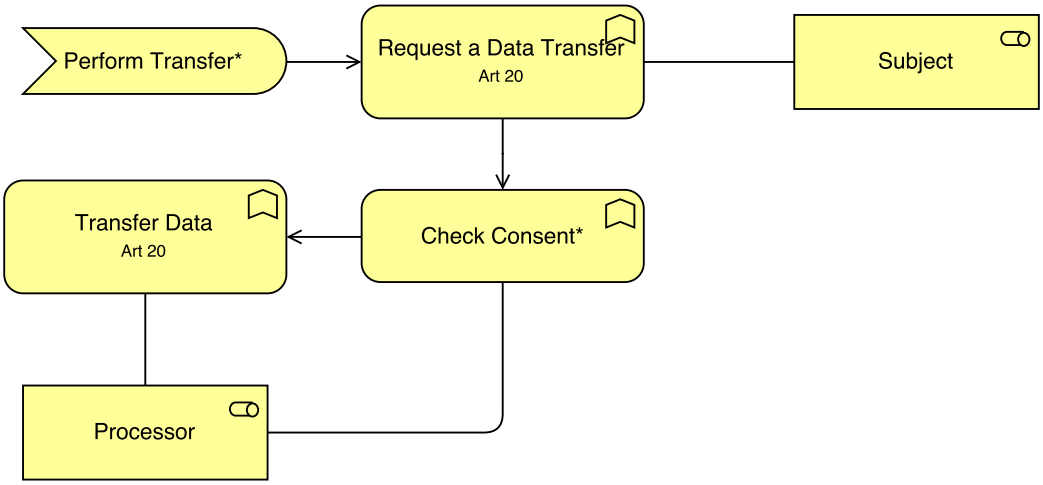

FIGURE 4.8 – Modèle de processus de transfert de données

6.3.4 Description du modèle de fonctions

Le modèle de fonctions (figure 4.9) représente l'ensemble des capacités des rôles qui existent pour le GDPR et, dans ce cas, qui concernent le consentement. Ces fonctions ou capacités sont celles utilisées dans les diagrammes d'activité.

7 Exploration d'un second principe : minimisation et nécessité

Suite à la modélisation du premier principe, le principe de **minimisation et necessité** est exploré.

La discussion de ce principe est moins exhaustive. Le but de cette section est de développer un autre modèle de la même manière afin d'éprouver la méthodologie.

7.1 Motivation

Ce second principe a été choisi car il est cités de nombreuses fois dans l'analyse faite à la section 3. De plus, son étendue est moins importante que le consentement, ce qui le rend plus facile à intégrer au premier modèle.

Définition : par minisation et nécessité s'entend le fait de récolter le moins de données possibles, donc de collecter uniquement les données qui sont nécessaires (à la réalisation d'un contrat par exemple).

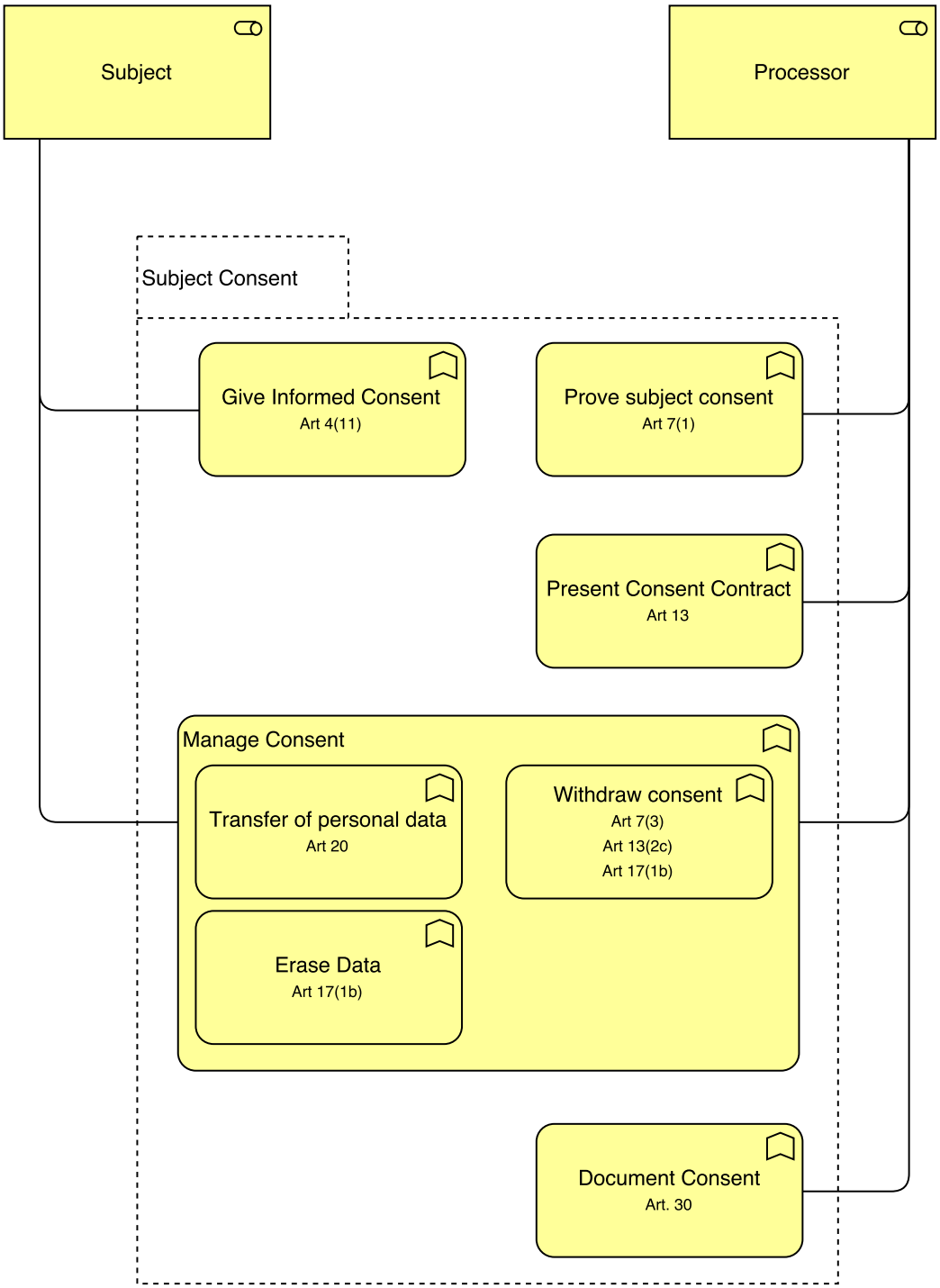

FIGURE 4.9 – Modèle de fonctions du consentement

7.2 Méthodologie de recherche sur la minimisation et la nécessité

La méthodologie sera sensiblement la même que celle présentée à la section 4.2 à ceci près que les deux premiers points qui concernent la recherche dans le guide et celle dans le texte légal même sont fusionnés car l'étendue du principe est moins grande.

7.3 Recherche dans le GDPR

Cette section est séparée en deux points : une concerne le terme de "minimisation" et l'autre de "nécessité". Les concepts restent fortement liés mais les termes sont différenciés dans le GDPR donc il convient de les aborder séparément dans un premier temps.

7.3.1 Recherche de minimisation

Les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire dans la réalisation de l'objectif. Art. 5(1c)

Le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées qui sont destinées à mettre en application les principes relatifs à la protection des données, comme la minimisation des données. Art. 25(1)

7.3.2 Nécessité

Pour qu'un traitement soit licite il faut, soit le consentement de la personne concernée (art. 6a), soit il faut que : Art. 6(b-f)

- Le traitement soit nécessaire à la réalisation d'un contrat ou préparer un contrat, ou
- Le traitement soit nécessaire à une obligation légale, ou
- Le traitement soit nécessaire à un intérêt vital pour la personne concernée, ou
- Le traitement soit nécessaire pour réaliser une tâche d'intérêt public ou d'une autorité officielle, ou
- Le traitement soit nécessaire à des buts d'intérêt légitime.

Un intérêt légitime n'est pas défini spécifiquement dans l'article, mais les considérants 47 à 50 donnent des exemples :

- Traitement pour du marketing direct ou pour la prévention de la fraude (47)
- Transmission de données à des buts d'administration interne (48)

— Assurance de la sécurité réseau et de l'information (49)
— Rapport de menace ou d'acte criminel (50)

Il est interdit, sauf sous au moins une des conditions ci-après, de traiter des données personnelles sensibles. Les conditions possibles sont les suivantes :

— Nécessaire pour l'emploi, la sécurité sociale ou la protection sociale ; art 9(2b)
— Nécessaire pour protéger les intérêts vitaux d'un sujet qui est légalement ou physiquement incapable de donner son consentement ; art 9(2c)
— Nécessaire pour des raisons judiciaires ; art 9(2f)
— Nécessaire pour des raisons établies par le pays membre ; art 9(2g)
— Nécessaire pour des raisons liées à la santé ; art 9(2h)
— Nécessaire pour des raisons liées à la santé et d'intérêt public ; art 9(2i)
— Nécessaire pour des objectifs d'archives ; art 9(2j)

Les restrictions sur les décisions basées uniquement sur les traitements automatisés (qui peuvent être du profilage) s'appliquent si le traitement produit des effets légaux ou des effets similaires. Ces traitements peuvent être utilisés si, notamment, ils sont nécessaires au traitement d'un contrat entre le contrôleur et le sujet. Art. 22(2a)

7.4 Recherche dans la littérature scientifique

La minimisation et la nécessité sont des concepts assez simples à appréhender et ne soulèvent pas de grandes questions dans la communauté scientifique. La revue de la littérature n'a rien apporté, en tout cas au niveau de la vie privée.

Une des raisons est peut-être que ces considérations ne concernent que le niveau business, et que l'implémentation est finalement assez simple à mettre à place : il s'agit de déterminer quelles données vont être collectées et si elles sont nécessaires. Le problème se résume globalement à cela.

Il existe néanmoins quelques articles qui évaluent la propension des personnes à donner plus d'informations sensibles que nécessaires suivant divers contextes ; comme Tourangeau et Smith [46] qui présentent une estimation de la quantité d'informations sensibles données par une personne concernée suivant trois contextes : des interviews personnelles assistées par ordinateur, des interviews remplies par la personne assistée par ordinateur et enfin des interviews audio remplies par la personne assistée par ordinateur. Mais cette étude n'est pas exploitable pour ce modèle car elle ne se base que sur des informations sensibles d'un seul type. De plus, elle reste encore expérimentale et manque de recul pour pouvoir en tirer des conclusions pour la construction

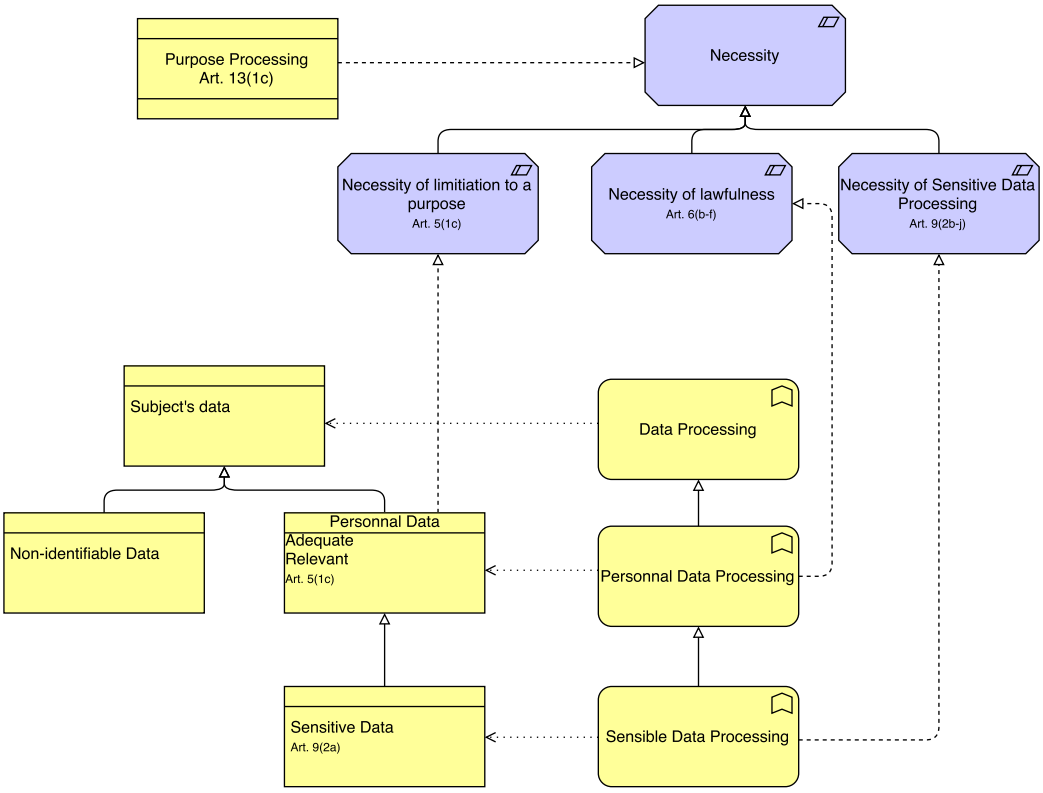

FIGURE 4.10 – Modèle actif et passif du principe de minimisatin et de nécessité

d'un modèle.

8 Modélisation du principe de minimisation et de nécessité

Un seul modèle est créé pour ce principe. Il intègre les structures actives et passives.

La figure 4.10 représente ce modèle.

D'abord d'un point de vue passif, les données du sujet peuvent être de deux types : des données non-identifiables ou des données personnelles. Les données personnelles doivent être adéquates, pertinentes et sont limitées à un objectif. Enfin, les données personnelles peuvent être des données sensibles.

D'un point de vue actif, il existe des fonctions pour traiter des données, mais également des fonctions pour traiter spécifiquement des données personnelles, voire des données sensibles.

Une partie du modèle utilise la couche ”motivation” afin de modéliser la nécessité. La nécessité est représentée comme une contrainte, puisque qu'elle est contrainte par le GDPR auprès des entreprises. La nécessité peut être de trois types : la limitation à un objectif, la léicité et le traitement des données sensibles. Afin de ne pas alourdir le modèle, le détail de ces nécessités n'a pas été modélisé (se référer à la section 7.3.2 pour le détail). Il est à noter que le traitement des données doit se référer à la nécessité, d'où le lien de réalisation entre les deux éléments.

9 Modèle intégré des deux modèles de principes

La dernière étape de la méthodologie consiste à intégrer tous les modèles issus de l'analyse par principe.

Seul le modèle statique du consentement est intégré à ce modèle car les autres (modèles de fonction et de processus) n'apportent rien d'intéressant à l'intégration puisque le modèle de minimisation et de nécessité ne comportent pas d'intersection avec ces modèles.

Le modèle intégré des principes de consentement et de minimisation et de nécessité se trouve à la figure 4.11

Dans ce modèle intégré, la structure des données de la personne concernée principalement est impactée. Il y a une fusion avec les deux modèles puisque les données de production peuvent se distinguer en données non-identifiables ou en données personnelles, tel que défini dans le modèle de minimisation et de nécessité. Les autres liens restent identiques.

9.1 Discussion sur le modèle intégré

Le modèle intégré montre que le recouvrement des principes permet effectivement de créer un modèle sur base de ces-dits principes pour le GDPR.

La forme du modèle ne permet pas de voir facilement la structure en couches sous-jacente. En effet, les éléments de motivation (la nécessité et ses spécialisations) ainsi que tous les éléments de contrat se trouvent dans la couche motivation, puisqu'ils ne représentent pas directement les éléments business.

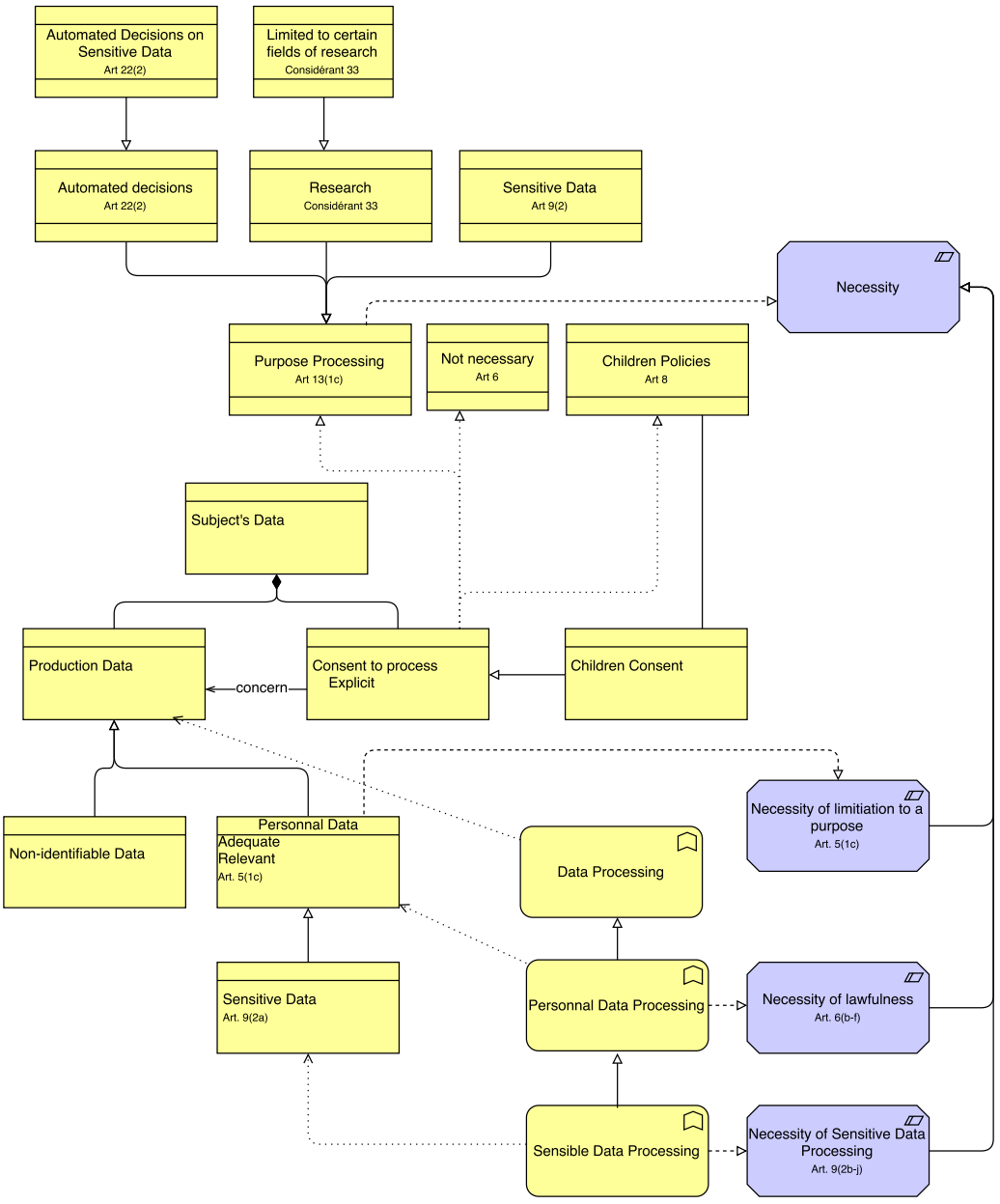

FIGURE 4.11 – Modèle intégré des principes de consentement et de minimisation et de nécessité

Chapitre 5

Discussion et conclusion

1 Discussion et conclusion

Ce mémoire présente une méthodologie de modélisation de textes légaux au niveau business, ainsi qu'une application concrète de cette méthodologie au "Règlement général sur la protection des données" [2]. Il s'inscrit dans une recherche de modélisation de la vie privée, en collaboration avec le LIST.

La méthodologie s'appuie sur une structure en couches d'abstraction telle qu'elle est définie dans Archimate 3.0[1], qui est utilisé comme outil de modélisation dans ce mémoire. Les couches définies par ArchiMate sont les suivantes : business, application et technologie (chapitre 1). Néanmoins, ces couches ont été adaptées à la méthodologie en considérant la motivation comme une couche au-dessus de la couche business, elle représente l'aspect légal.

L'état de l'art (chapitre 2) a présenté la vie privée sur les couches les plus basses (applicatives) et plus hautes (motivation-business), suivi d'une revue de différents langages de modélisation au niveau business mais pouvant s'étendre sur plusieurs couches. La dernière partie de l'état de l'art a mis en évidence diverses manières de modéliser les textes légaux au niveau business. Cette partie a mis en évidence que les frameworks de modélisation de textes légaux sont généralement orienté processus, c'est-à-dire qu'ils cherchent à créer des modèles de "comportement". D'autre part, ces frameworks présentent souvent (50% dans cet état de l'art) une implémentation dans le domaine de la santé. Il est vrai que la santé est un domaine sensible pour les données, cela explique problablement une littérature plus importante à ce sujet. Néanmoins, ils peuvent être moins adaptés à un contexte plus général de protection des données, tel que mis en oeuvre par le GDPR.

La méthodologie développée au chapitre 3 se base sur un premier méta-

modèle, qui a ensuite été affiné, sur base d'une première idée non raffinée, en un second méta-modèle. Ce dernier a servi de base pour cette méthodologie.

La première partie de la méthodologie est d'extraire les concepts légaux. Divers auteurs présentent des manières systématiques et formelles pour extraire les concepts légaux. Cette méthodologie n'impose pas de méthode particulière. Dans le cadre de l'application de cette méthodologie, un Mind-map a été mis en oeuvre pour représenté l'extraction des "éléments légaux".

La seconde partie est la modélisation **orientée-principes** qui consiste à identifier les principes du domaine —la vie privée dans ce cas— dans la littérature et les standards, de classifier les éléments légaux dans ces catégories puis de les modéliser principe par principe.

Durant tous les processus d'extraction et de modélisation, il convient de conserver une traçabilité des articles.

Dans ce mémoire, l'application de la méthodologie n'a été effectuée que sur deux principes. Les résultats sont assez intéressants puisqu'ils montrent une bonne corrélation entre les principes et le légal, ce qui renforce l'hypothèse de double-validation (chapitre 3 section 5). Ces résultats sont donc encourageants, mais il faut tout de même noter que l'application à seulement deux principes n'est pas suffisante pour affirmer avec certitude la validité de cette méthodologie. Dans le cas où tous les éléments légaux liés à tous les principes seraient modélisés, il peut rester, d'une part comme de l'autre (dans les principes ou dans le texte légal), des éléments non-traités. Comment les modéliser et les intégrer à cette méthodologie ?

2 Travaux futurs

Les travaux futurs sont liés à la question de la section précédente. Dans le futur, il s'agira de tester cette méthodologie sur un texte légal en entier, mais également sur un autre texte que seul le GDPR.

D'autre part, il serait également possible de tester d'autres types d'extraction des concepts légaux, voire des principes, afin de les confronter à ceux de ce mémoire. Et notamment, adapter des frameworks existants, comme celui de la thèse de Ghanavati [18] discuté à la section 6.2 du chapitre 3.

Enfin, la modélisation devrait être améliorée avec un processus systématique plus formel.

Annexe A

Veille sur les processus de consentement

1 Introduction

L'objectif de cette veille est de présenter les processus mis en place par différentes institutions, standards ou auteurs afin d'obtenir et de traiter le consentement des sujets des données.

Il est à noter que, à l'heure actuelle, de tels processus sont mis en place presqu'exclusivement dans le milieu de la santé ou de la recherche. Or, ce travail porte sur le GDPR qui concerne le traitement de tout type de donnée à caractère personnel. Il faut donc être vigilant quant à la valeur des éléments suivants.

2 Définition

Processus d'obtention du consentement = processus business décrivant une suite d'étapes permettant d'obtenir le consentement éclairé du sujet.

3 University of Nebraska

L'université du Nebraska, sur son site internet [1], donne des conseils sur le consentement, et notamment sur les processus pour obtenir ce consentement.

1. http://www.unk.edu/academics/gradstudies/irb/consent-assent/process-for-obtaining-informed-consent.php

Auteur	University of Nebraska Kearney
Titre	Process for Obtaining Informed Consent
Année	Inconnue
Origine	USA
Contexte	Recherche

Voici une citation du site avec des éléments de processus mis en évidence :

"During the process of informed consent, **all Elements of the Consent Form should be carefully, patiently, and clearly explained** to the prospective subject. In addition, the researcher should frequently assess the prospective subject's **understanding** by asking appropriate questions. During the process for enrolling a subject in non-Exempt research, the investigator should **explain to the subjects their Rights** as Research Participants. The explanation of a research subject's rights is considered an adjunct to informed consent and demonstrates the commitment of both the researcher and the university to the conduct of human subject research with the highest integrity and skill possible. The IRB encourages researchers to provide their subjects with a written copy of the UNK's Rights of Research Subjects. The following are general guidelines for writing the consent form, the required elements that should be included in all consent forms, and the characteristics of each element based on level of risk with samples".

4 ACRP

L'ACRP ou *The Association of Clinical Research Professionals* est une association basée à Washington qui travaille sur la recherche clinique. Elle a écrit un *White Paper* [34] sur le processus du consentement informé dans ce contexte.

Auteur	ACRP
Titre	The Process of Informed Consent
Année	2013
Origine	USA
Contexte	Santé

Voici le processus qu'elle donne pour obtenir le consentement :

1. Assurer que l'environnement convient.
2. Assurer que la personne a la capacité de consentir, c'est-à-dire la capacité cognitive et légale de fournir un consentement informé.

3. Les éléments du consentement doivent être présentés et discutés avec le sujet d'une manière séquentielle. Il est également conseillé de poser des questions ouvertes au sujet pour vérifier sa compréhension.
4. Le temps entre la présentation des éléments et le consentement peut être plus ou moins grand suivant la nature des éléments. Dans le cas de consentement portant sur un élément important ou risqué, une procédure de consentement décalé peut être envisagée pour laisser le temps au sujet de réfléchir à son consentement.
5. Assurer la compréhension du sujet. Une méthode possible est de proposer un test avec des questions à choix multiples afin d'évaluer la compréhension du sujet.
6. Documenter le consentement informé
7. Redemander le consentement du sujet au cours du temps, en cas de modification ou après une longue période.

5 CNO

Dans un contexte similaire à l'ACRP, le CNO [2] (ou OIIO en français) est l'instance dirigeante des infirmières en Ontario (Canada). Parmi ses rôles, l'un d'entre eux est d'articuler et promouvoir des standards de pratique [35].

Auteur	CNO
Titre	Consent
Année	2013
Origine	Canada
Contexte	Santé

Il a mis en ligne un document de guideline de pratiques sur le consentement, dans lequel il donne divers informations sur le consentement : définitions, point de vue légal... etc. Et notamment, on y trouve des étapes d'obtention du consentement.

1. Évaluer la capacité du sujet à consentir
2. Fournir un traitement d'urgence ou une admission en cas de crise
3. Informer le patient qu'une personne prendra la décision à sa place
4. Identifier une personne de substitution pour prendre la décision
5. Obtenir le consentement de la personne de substitution

2. http://www.cno.org/en/what-is-cno/

Ce processus de consentement s'applique uniquement en milieu hospitalier et dans le cas très précis de soin de santé par un professionnel de la santé. D'autre part, ce processus n'est pas un ensemble d'étapes pour obtenir le consentement du sujet, mais toutes les étapes pour obtenir un consentement, dans le cas où, passé l'étape 1, le sujet ne serait pas capable de le donner lui-même.

6 CHI

Le CHI (*Centre for Healthcare Improvment*) est l'initiative du gouvernement australien. Leur guide *Guide to Informed Decision-making in Healthcare* [27] est un guide de bonnes pratiques cliniques, dans lequel on trouve un point concernant le processus à suivre pour obtenir le consentement.

Auteur	CHI
Titre	Guide to Informed Decision-making in Healthcare
Année	2012
Origine	USA
Contexte	Santé

Voici le processus qu'ils donnent pour obtenir le consentement :

1. Evaluer les infos que doit avoir le sujet
2. Fournir suffisamment d'informations pour que le sujet puisse prendre une décision éclairée
3. Evaluer le niveau de détail auquel l'information est fournie au sujet
4. Présenter l'information
5. Vérifier la compréhension par le sujet
6. Obtenir le consentement
7. Documenter le consentement

7 OHRPP

L'*Office of the Human Research Protection Program* (OHRPP) est une organisation américaine qui fournit un leadership dans la protection des droits et du bien-être des personnes impliquées dans des recherches conduites ou supportées par les USA. Ils ont créé un document [36] donnant des informations sur la manière d'obtenir le consentement éclairé de sujets d'études.

Auteur	OHRPP
Titre	Guidance and Procedure : Obtaining and Documenting Informed Consent
Année	2011
Origine	USA
Contexte	Recherche

Processus d'obtention du consentement :

1. Expliquer la recherche
   (a) Expliquer l'étude
   (b) Présenter le contrat de consentement et laisser le temps à la personne concernée pour réfléchir
   (c) Répondre aux éventuelles questions
2. Assurer la compréhension de la personne concernée : poser des questions ouvertes pour assurer qu'elle a bien compris

Bibliographie

[1] ArchiMate® 3.0 Specification. `http://pubs.opengroup.org/architecture/archimate3-doc/chap06.html`. Accédé le 21/04/2017.

[2] General Data Protection Regulation, April 2016.

[3] Annie I. Antón, Elisa Bertino, Ninghui Li, and Ting Yu. A roadmap for comprehensive online privacy policy management. *Communications of the ACM*, 50(7) :109–116, 2007.

[4] C.A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati. A privacy-aware access control system. *Journal of Computer Security*, 16(4) :369–397, July 2008.

[5] Claudio Agostino Ardagna, S. De Capitani di Vimercati, and Pierangela Samarati. Enhancing user privacy through data handling policies. In *IFIP Annual Conference on Data and Applications Security and Privacy*, pages 224–236. Springer, 2006.

[6] Paul Ashley, Calvin Powers, and Matthias Schunter. From privacy promises to privacy management : a new approach for enforcing privacy throughout an enterprise. In *Proceedings of the 2002 workshop on New security paradigms*, pages 43–50. ACM, 2002.

[7] Ruth Boardman, James Mullock, and Ariane Mole. Bird & Bird Guide to the General Data Protection Regulation, April 2016.

[8] Travis D. Breaux, Matthew W. Vail, and Annie I. Anton. Towards regulatory compliance : Extracting rights and obligations to align requirements with regulations. In *Requirements Engineering, 14th IEEE International Conference*, pages 49–58. IEEE, 2006.

[9] Ann Cavoukian, Scott Taylor, and Martin E. Abrams. Privacy by Design : essential for organizational accountability and strong business practices. *Identity in the Information Society*, 3(2) :405–413, August 2010.

[10] Sabrina De Capitani Di Vimercati, Sara Foresti, Giovanni Livraga, and Pierangela Samarati. Data privacy : Definitions and techniques. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 20(06) :793–817, 2012.

[11] Josep Domingo-Ferrer. A Three-Dimensional Conceptual Framework for Database Privacy, May 2008.

[12] Matt Duckham and Lars Kulik. A formal model of obfuscation and negotiation for location privacy. In *International Conference on Pervasive Computing*, pages 152–170. Springer, 2005.

[13] Wilco Engelsman, Dick Quartel, Henk Jonkers, and Marten van Sinderen. Extending enterprise architecture modelling with business goals and requirements. *Enterprise Information Systems*, 5(1) :9–36, February 2011.

[14] Hans-Erik Eriksson and Magnus Penker. Business modeling with UML. *New York*, 2000.

[15] Parlement Européen. Nouvelle législation européenne sur la protection des données. `http://www.europarl.europa.eu/news/fr/news-room/20160413BKG22980/nouvelle-l%C3%A9gislation-europ%C3%A9enne-sur-la-protection-des-donn%C3%A9es`. Accédé le 08/04/2017, Publié le 01/06/2016.

[16] Christophe Feltus, Eric Grandry, Thomas Kupper, and Jean-Noël Colin. Model-driven Approach for Privacy Management in Business Ecosystem. *Modelsward 2017*, pages 392–400, 2017.

[17] Boris Fritscher and Yves Pigneur. Business IT Alignment between Business Model and Enterprise Architecture with a Strategic Perspective. *International Conference on Advanced Information Systems Engineering*, pages 4–15, June 2011.

[18] Sepideh Ghanavati. *Legal-URN Framework for Legal Compliance of Business Processes*. PhD thesis, University of Ottawa, 2013.

[19] Sepideh Ghanavati, Daniel Amyot, and Liam Peyton. A Requirements Management Framework for Privacy Compliance. In *WER*, pages 149–159. Citeseer, 2007.

[20] Sepideh Ghanavati, Daniel Amyot, and Liam Peyton. A Requirements Management Framework for Privacy Compliance. In *WER*, pages 149–159. Citeseer, 2007.

[21] Sepideh Ghanavati, Daniel Amyot, and Liam Peyton. Compliance analysis based on a goal-oriented requirement language evaluation methodology. In *Requirements Engineering Conference, 2009. RE'09. 17th IEEE International*, pages 133–142. IEEE, 2009.

[22] Jaap Gordijn, Hans Akkermans, and J. Van Vliet. Designing and evaluating e-business models. *IEEE intelligent Systems*, 16(4) :11–17, 2001.

[23] Jaap Gordijn, Eric Yu, and Bas van der Raadt. E-service design using i* and e/sup 3/value modeling. *IEEE software*, 23(3) :26–33, 2006.

[24] Paolo Guarda and Nicola Zannone. Towards the development of privacy-aware systems. *Information and Software Technology*, 51(2) :337–350, February 2009.

[25] Wesley Hohfeld. Fundamental legal conceptions. *New Haven : Yale University Press*, 1919.

[26] Adnan Imeri, Abdelaziz Khadraoui, André Rifaut, and Damien Nicolas. The new strategy to develop scenarios in compliance with legal and ethical issues. 2016.

[27] Informed Consent Program Manager Patient Safety and Quality Improvement Service Centre for Healthcare Improvement. Guide to Informed Decision-making in Healthcare.

[28] Marc Langheinrich. Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing*, pages 273–291. Springer, 2001.

[29] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. t-closeness : Privacy beyond k-anonymity and l-diversity. In *Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on*, pages 106–115. IEEE, 2007.

[30] Ruopeng Lu, Shazia Sadiq, and Guido Governatori. Measurement of Compliance Distance in Business Processes. *Information Systems Management*, 25(4) :344–355, October 2008.

[31] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. *L* -diversity : Privacy beyond *k* -anonymity. *ACM Transactions on Knowledge Discovery from Data*, 1(1) :3–es, March 2007.

[32] Marco Casassa Mont, Siani Pearson, Gina Kounga, Yun Shen, and Pete Bramhall. On the Management of Consent and Revocation in Enterprises : Setting the Context. *HP Laboratories, Technical Report HPL-2009-49*, 2009.

[33] Marco Casassa Mont and Vaibhav Sharma. EnCoRe : dynamic consent, policy enforcement and accountable information sharing within and across organisations. *HP Laboratories technical Report# : HPL-2012-36*, 2012.

[34] Association of Clinical Research Professionals. White Paper - The Process of Informed Consent, April 2013.

[35] College of Nurses of Ontario. Consent - Practice Guideline, 2009.

[36] Office of the Human Research Protection Program. Obtain Informed Consent, July 2011.

[37] Alexander Osterwalder and Yves Pigneur. *Business model generation : a handbook for visionaries, game changers, and challengers.* John Wiley & Sons, 2010.

[38] Siani Pearson and Marco Casassa Mont. Sticky policies : An approach for managing privacy across multiple parties. *Computer*, 44(9) :60–68, 2011.

[39] Pablo A. Pérez-Martínez and Agusti Solanas. W3-privacy : the three dimensions of user privacy in LBS. In *Proceedings of12th ACM International Symposium on Mobile Ad Hoc Networking and Computing. Paris : ACM*, 2011.

[40] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization : Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. 2010.

[41] Pierangela Samarati. Protecting respondents identities in microdata release. *IEEE transactions on Knowledge and Data Engineering*, 13(6) :1010–1027, 2001.

[42] Alberto Siena, Anna Perini, Angelo Susi, and John Mylopoulos. A Meta-Model for Modelling Law-Compliant Requirements. pages 45–51. IEEE, September 2009.

[43] Alberto Siena, Anna Perini, Angelo Susi, and John Mylopoulos. Towards a framework for law-compliant software requirements. In *ICSE Companion*, pages 251–254, 2009.

[44] Daniel J. Solove. Privacy self-management and the consent dilemma. 2012.

[45] Latanya Sweeney. k-anonymity : A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05) :557–570, 2002.

[46] Roger Tourangeau and Tom W. Smith. Asking Sensitive Questions : The Impact of Data Collection Mode, Question Format, and Question Context. *Public Opinion Quarterly*, 60(2) :275, 1996.

[47] Azmat Ullah and Richard Lai. Modeling business goal for business/IT alignment using requirements engineering. *Journal of Computer Information Systems*, 51(3) :21–28, 2011.

[48] William M Ulrich and Philip Newcomb. *Information systems transformation : architecture-driven modernization case studies*. Morgan Kaufmann, 2010.

[49] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-preserving public auditing for data storage security in cloud computing. In *Infocom, 2010 proceedings ieee*, pages 1–9. Ieee, 2010.

[50] Edgar A. Whitley. Informational privacy, consent and the "control" of personal data. *Information security technical report*, 14(3) :154–159, 2009.

[51] Eric Yu, Paolo Giorgini, Neil Maiden, and John Mylopoulos. 1 Social Modeling for Requirements Engineering : An Introduction. *Social Modeling for Requirements Engineering*, pages 3–10, 2011.

[52] Eric SK Yu. Towards modelling and reasoning support for early-phase requirements engineering. In *Requirements Engineering, 1997., Proceedings of the Third IEEE International Symposium on*, pages 226–235. IEEE, 1997.